CVR / IT Consulting

Commitment – Vision - Results

Office: (919) 495-7371
FAX: (919) 556-0283
Email: info@cvr-it.com
Web: www.cvr-it.com

Elevator/Amusement Project Business Analysis Report

Version 1.9

Elevator System

Prepared for State of North Carolina Department of Labor

by CVR/IT Consulting LLC

Author: Gary J. Evans

CVR/IT Consulting LLC

CVR/IT Consulting LLC provides guidance and support in the effective use of Project, Program and Portfolio Management Technologies, including Business Analysis process and technique and development of the Project Management Office. The company, founded in May, 2002, is owned and operated by Dr. Gary J. Evans, PMP. CVR/IT Consulting LLC provides professional consultation in all matters related to Project Management and Business Analysis.

If there are any questions about the assessment described in this report, Dr. Evans can be reached at:

Phone: (919) 495-7371

Email: gary.evans@cvr-it.com

Table of Contents

I. Description of the Elevator/Amusement Project

A. Goals of the project

The Elevator and Amusement Device Bureau is responsible for the proper installation and safe operation of all elevators, escalators, workman's hoists, dumbwaiters, moving walks, aerial passenger tramways, amusement rides, incline railways and lifting devices for persons with disabilities that operate in public establishments (except federal buildings) and private places of employment. More than 28,000 inspections are conducted annually by the Bureau, which first undertook its periodic safety code inspection program in 1938.

1. Elevator System Description
   The Bureau currently uses a custom software system to support its elevator operations. The current system is limited in function and interfaces with other bureaus are primitive (i.e. spreadsheets) and labor intensive. The Bureau has decided to replace the existing Elevator System with a more full-featured one in order to improve the effectiveness of the Bureau and support the expected growth in number of elevator inspections without increasing the number of Inspectors and Support Staff.

2. Amusement Device System Description
   The Bureau currently has no formal software system to support its amusement device operations. Currently, Bureau Staff use a combination of spreadsheets and manual process to plan work, collect and process data, and report on work accomplished. The Bureau has decided to develop a full-featured Amusement Device System in order to improve the effectiveness of the Bureau, provide better service to the public and increase the overall safety of amusement rides used in NC.

The long term business value expected from this project includes:

1. Improved safety that results in fewer injuries and fatalities
2. More effective inspection techniques due to access to better data, as measured by better ability to find defects and, in some cases, in less time
3. Information sharing (two-way) with other states to improve safety
4. The System will provide important information for use in training

B. Goals of this analysis

This analysis pertains to the Elevator System only. The Bureau intends to use a highly configurable Commercial Off The Shelf System (COTS) that will fully support its elevator inspections. This COTS system will be procured via a request for proposals (RFP) issued through the Office of the State Controller. The Bureau understands the importance of developing sufficient requirements information so that a Vendor can fully understand what is required and thereby develop a high quality system. This document will be made available to Vendors as supplemental information to the RFP.

This document contains the results of a brief business analysis of the Bureau's intentions with respect to a future system. Requirements presented here are intended to:

- Describe the majority of required system functions
- Provide examples of use cases, reports and other detail that Vendors may find useful
- Reveal some of the most pressing issues that must be resolved before a new system can be configured

This document is not intended to be all inclusive, and it leaves many questions unanswered. ***These unanswered questions should be addressed during the business process reengineering effort expected to follow as part of the awarded Vendor's deliverables.***

II. High level Business Requirements – Elevator System

Business requirements are those features, functions, capabilities and conditions that project deliverables must provide if the project is to deliver the business value intended. Business requirements drive the requirements process; all functional requirements must tie back to at least one business requirement. At the end of the project, deliverables should be validated to demonstrate that they have met the business requirements.

In order to deliver the business value expected of this project, the new Elevator System must meet the following high level business requirements.

a. Be flexible, including but not limited to the following:
    1. Allow addition of new device types, operation types, inspection types, violation codes
    2. Allow addition of new fees and penalties and tracking of payments (and non-payments)
    3. Allow defined user types/roles with different levels of access (e.g. Customer; Inspector; Back Office; System Administrator)
    4. Support multiple types of inspection, including new device, routine, special, alteration and compliance
    5. Support many types of devices, including for example elevators, lifts and escalators
    6. Support multiple permit types, including new, modification and repair
    7. Provide a useful array of predefined reports and allow creation of new reports
b. Be easy to use, as defined by Users of the System, e.g.
    1. Dropdown lists whenever entries can be pre-defined
    2. Cascading dropdown lists so that, for example, what appears in the second list depends on what was selected in the first
    3. The ability to easily maintain dropdown lists
    4. Automatic error checking when possible to ensure data consistency
    5. Perform functions with a minimum number of steps
    6. Minimum redundant data entry
    7. Make it easy to:
        a) Work with inspector and supervisor data (e.g. create and assign new Inspectors)
        b) Equitably assign devices to Inspectors
        c) Review inspection results
        d) Review inspector work metrics (e.g. for one day the number of inspections, hours spent in travel, hours spent in conference)
c. Support reporting:
    1. Allow ad hoc reporting on all available data
    2. Allow creation of canned reports (i.e. with built-in selection criteria)
    3. Allow creation of pre-defined reports with user-selectable criteria
    4. Provide automated delivery of reports on a timed (e.g. daily or weekly) basis (e.g. list of overdue invoices)
    5. Be able to generate and save reports in multiple formats (e.g. PDF, comma-delimited and Excel)
    6. Control which user roles can run which reports
    7. Provide an array of reports (defined by the Bureau) in the delivered System
d. Provide a means for each User to receive documents and messages from the System. For example, the System can provide a My Communications feature which allows the User to see reports, messages from the System and other Users, and other information.
e. Provide a means (e.g. a comments capacity) so that Users can enter, track and share information related to inspections, invoices, late payments, etc.)

f. Support the work of Field Inspectors:
    1. Give Inspectors access to all device data, including previous inspection reports
    2. Allow effective data sharing between the main System and Inspectors in the field
    3. Provide a means for Inspectors to determine the most efficient travel route for a specified set of inspections
    4. Allow the Inspector to indicate the violation code reference document in effect at the time of device acceptance or alteration
    5. Support tracking of variances from the violation code reference document
    6. Provide a simple process that keeps data concurrent between Inspectors and the Back Office
    7. Support field printing of certificates, inspection reports and other documents
    8. Support field scanning of documents and upload into the System
    9. Support upload of digital photos into the System
g. Support assigning and tracking of violation abatements
h. Support investigations, including storage and easy access to photos and other non-text materials
i. Provide a public interface, e.g. web portal:
    1. Allow Customers to submit permit applications and other communications with Bureau Staff, with automatic saving of customer data into the System
    2. Support secure ID and password for Users of the public interface
    3. Allow use of paper forms when a Customer does not have access to the public interface (i.e. Back Office Personnel can enter data for the applicant)
j. Support all relevant business rules found in the Elevator Safety Act
k. Include the ability to store and display a library of reference documents (PDF format) used by Inspectors
l. Support multiple address types, including Applicant, Owner, Physical Address, Local Contact, Billing, Maintenance, and Property Management
m. Support Freedom of Information Act (FOIA) and NC Public Records Act requests
n. Support tracking of manufacturer recalls
o. Support interface with the Budget Office:
    1. Create and deliver invoices
    2. Support separate processes for payment by check, eCheck, credit card and ACH
    3. Support tracking of checks returned due to non-sufficient funds (an “NSF check”)
    4. Allow correction of incorrect payments
    5. Support tracking of payments of fees and penalties separately
p. Support integration with Microsoft Active Directory
q. Maintain an audit trail of all data changes
r. Maintain a history of all data changes
s. Support multiple roles

III. Use Cases

A use case is a description of how a User interacts with the System. Each use case scenario provides a description of how one or more predefined actors (e.g. Inspector, Back Office Staff) interact with the System to accomplish a single business function. The following is a list of known use case scenarios that must be supported in the new System.

The use cases presented here are intended to provide an understanding of the range and level of complexity of planned system operations. The use cases are not in standard use case scenario format, as they contain a blend of business and system use case scenario characteristics. While trigger, actor(s) and high-level primary workflow descriptions are provided for each use case, not all alternative and exception flows, artifacts or other details are included. ***It is expected that these details will be defined during the detailed requirements analysis of the implementation project as performed by the awarded Vendor.***

A. Inspectors

1. The Inspector performs an inspection of a new device – Standard Certificate
   When a new device such as an elevator or escalator is fully installed, the Installer (i.e. Elevator Company) can submit a request for an inspection. The Inspector does an inspection and provides a certificate of operation if the inspection passes. This allows the Installer to activate the device.
   a. This use case is triggered when:
      1) The Installer uses the public interface to inform NCDOL that a new equipment installation is complete, and
      2) The Installer desires a standard certificate, and
      3) The Inspector has arrived at the site
   b. The Inspector logs onto the System and selects the **Inspect New Device** function.
   c. The System prompts for a **State ID#**.
   d. The Inspector enters a **State ID#**.
   e. The System displays device information for that **State ID#**.
   f. If this is the initial inspection:
      1) Inspector reviews data, then selects the **New Inspection Data Entry** function.
      2) System displays the new inspection data entry screen, including an inspection checklist specific for the device being inspected.
         a) The System displays information about any variance(s) that may have been granted so that the Inspector can check to be certain that terms of the variance have been followed (e.g. necessary work has been done).
      3) Inspector may refer to code reference documents available through the System (see Inspector Library below) while doing the inspection. These include, for example:
         a) ASME codes
         b) NFPA codes
         c) Guides
      4) Inspector enters data relevant to the inspection (e.g. violations found, optional note on each violation).
      5) Inspector indicates that data entry is complete.
      6) There is a fee for this and any subsequent new device inspections that may be necessary.
         a) The billing address for new device inspection is always the Elevator Company.
      7) System displays the record so that the Inspector can review it. Inspector may edit the content, save the record, save entered data for later completion or cancel.
         a) If the record is saved as complete, the Inspector prints an inspection report and gives it to the onsite customer contact (e.g. Elevator Company Representative).
         b) After completing and saving an inspection record, the Inspector can:
            a. Open the record for edit (e.g. to correct an error).
            b. Reprint the inspection report.
      8) If the inspection passed, Inspector prints a certificate of operation and installs it in the elevator.
         a) The Inspector indicates in the System that the certificate is in place.
         b) The System sets device status to **Active**.
      9) If there is ANY violation at any level the inspection does not pass and no certificate is issued. If the inspection does not pass due to one or more violations, the Inspector:
         a) Notes violations in the inspection report.

1. Report includes the name, title and phone number of the person the Inspector pointed the violation out to.
2. One inspection report can include many violations. Violation data includes code reference document number and narrative.
3. The System should allow at least 1024 characters for violation notes.

b) Gives the printed inspection report to the Installer and points out the violations.
c) Does NOT print a certificate of operation.

g. If this is not the initial inspection, e.g. violations were found in the initial inspection and this is a follow-up inspection:
   1) Inspector selects the **Update Ongoing Inspection** function.
   2) System displays data of the ongoing inspection.
   3) Inspector updates the record with current data based on the latest inspection.
   4) Remainder of the use case is as listed above.
h. End of use case.

2. The Inspector performs an inspection of a new device – 90-Day Certificate

When a new elevator has been installed, the Installer (i.e. General Contractor of Record) can submit a request for an inspection to activate the elevator on a limited basis. The Inspector does an inspection and provides a limited (i.e. 90-day) certificate if the inspection passes. This certificate allows the Installer to use the elevator for construction purposes. Such elevators may be only partially installed and missing something that does not create a safety issue.

a. This use case is triggered when:
   1) The Customer (i.e. General Contractor of Record) uses the public interface to inform NCDOL that a new equipment installation is under way, and
   2) Customer desires a 90-day certificate, and
   3) The Inspector has arrived at the site.
b. The Inspector logs onto the System and selects the **Inspect New Device** function.
c. Inspector enters data into the System as described above for Perform inspection of New Device – Standard Certificate.
d. There is a fee for this and all subsequent 90-day inspections:
   1) The billing address for 90-day certificate is always the Elevator Company.
e. If the Inspector finds that all primary functions work:
   1) The Inspector prints the 90-day certificate and posts it in the elevator.
   2) The System sets device status to **Limited**.
   3) The System prints out and gives the Installer a copy of a form that contains rules and regulations.
   4) The Installer posts the form in the elevator
   5) The Inspector indicates in the System who received the form.
f. If the Inspector finds any violations to prevent issue of a 90-day certificate, the Inspector notes violations in the System, prints an inspection report and gives it to the Installer. No certificate is issued.
g. At the end of 75 days if the Installer has not informed the Back Office or the Inspector that work on the elevator is completed:
   6) The System alerts the Inspector that the 90 day period will end in 15 days.
   7) The Inspector has the option of contacting the General Contractor of Record or the Elevator Company to find out if the work has been completed.
      a) If the work is not completed and the General Contractor of Record does not want an additional 90 days, the Inspector removes the certificate, and the System sets device status to **Decertified**.

b) If the General Contractor of Record takes no action and the 90-day certificate expires, the System alerts the Inspector, the Inspector removes the certificate, and the System sets device status to **Decertified**.
c) If the work is not completed and the General Contractor of Record wants an additional 90 days, the General Contractor of Record submits a request on the public interface.

h. The Elevator Company can request multiple 90-day extensions for use. The Inspector does a 90-day inspection as described above for each extension.
i. End of use case.

3. The Inspector cancels a new inspection request
   a. This use case is triggered when an Elevator Company of Record cancels a request for a new device inspection.
   b. Elevator Company contacts the Inspector to cancel the inspection.
   c. When Inspector learns of a cancellation, they:
      a. Select the **Cancel Inspection** function.
      b. Select the planned inspection.
      c. Enter the cancellation.
      d. System saves the data.
   d. System sends billing notice to Budget as follows:
      a. If Elevator Company cancels less than 24 hours of the planned inspection, they are billed for the inspection.
      b. If Elevator Company gives more than 24 hours notice, they are not billed.
   e. End of use case.
4. The Inspector performs a routine inspection
   a. This use case is triggered when:
      1) One year has passed since the last new, routine or alteration inspection, and
      2) The Inspector is onsite for the inspection.
   b. The Inspector logs onto the System and selects the appropriate function.
   c. The System prompts for a **State ID#**.
   d. The Inspector enters a **State ID#**.
   e. The System displays device information for that **State ID#**.
   f. Inspector reviews data, then selects the **Routine Inspection** function.
   g. System displays the routine inspection data entry screen.
      1) This includes an inspection checklist specific for the device being inspected.
      2) The System displays information about any variance(s) that may have been granted so that the Inspector is aware of them.
   h. Inspector may refer to reference documents available through the System while doing the inspection. These include, for example:
      1) ASME codes
      2) NFPA codes
      3) Guides
   i. Inspector enters data relevant to the inspection (e.g. violations found, with an optional note on each violation).
   j. Inspector indicates that data entry is complete.
   k. System displays the record so that the Inspector can review it. Inspector may edit the content, save the record, save entered data for later completion or cancel.
      1) If the record is saved as complete, the Inspector prints an inspection report and gives it to the Owner or Owner Representative.
      2) After completing and saving an inspection record, the Inspector can:
         a) Open the record for edit (e.g. to correct an error).
         b) Reprint the inspection report.
   l. There is a fee for this inspection.

m. Inspector verifies the bill-to address or updates the bill-to address. However any bill-to address entered by the Inspector is only temporary. This address must be verified by Budget before it can be used as the billing address.
n. If the device passed inspection, the Inspector signs the certificate of operation and places it back in the elevator or, if needed, prints a new certificate and signs it.
o. There are three levels of violation: **Minor**, **Significant** and **Imminent Threat To Public Safety**. When more than one level of violation is found, the Inspector uses the workflow associated with the most severe level.
    1) If the inspection does not pass due to a minor violation, the Inspector:
        a) Notes in the System that there is a minor violation.
        b) Sets an abatement date by which time violations must be fixed. This date can be 10, 20 or 30 days from the date of the current inspection.
        c) May indicate in the record that a compliance inspection is required when the violation is of sufficient severity (at the discretion of the Inspector). By default no compliance inspection is required if nothing more than a minor violation is found.
        d) Prints a copy of the finished report, gives it to the Owner or Owner Representative, and points out the violation(s).
        e) Signs the certificate or, if necessary, prints and signs a new one, and places it in the elevator.
    1) If the inspection does not pass due to a significant violation, the Inspector:
        a) Notes in the System that there is a significant violation.
        b) Prints an inspection report that includes a list of all violations.
            - Report includes the name, title and phone number of the person the Inspector pointed the violation out to, and the name of person who is responsible for fixing the violation.
            - The report can include one or many violations.
            - Violation data includes, for example, code number, code narrative and optional note. The System should allow at least 1024 characters for violation notes.
        c) Gives the printed inspection report to the Owner or Owner Representative and points out the violations.
        d) If the violation is of sufficient severity:
            - The Inspector removes the certificate of operation from the device.
            - The Inspector has the System print a shutdown order that includes a list of legal rights for specific violations.
            - The Inspector gives the shutdown order to the Owner or Owner Representative who signs the document.
            - The Inspector scans the document and attaches it to the record.
            - The System sets device status to **Shutdown**.
            - Inspector must return and the device must pass inspection before certificate can be signed and reissued.
        e) If there is no shutdown, the Inspector sets an abatement date by which time violations must be fixed. This date can be 10, 20 or 30 days from the date of the current inspection.
        f) When there is a shutdown order there cannot be an abatement.
        g) A compliance inspection is required whenever there are one or more significant violations found during a routine inspection. This is in contrast to a minor violation where the compliance inspection is optional.
    1) If the Inspector finds an imminent threat to public safety, the Inspector:
        a) Notes in the System that there is an imminent threat to public safety and

b) Takes all actions listed for significant violation and
c) Locks out the elevator.

2) In addition, the System sets device status to **Locked Out**.

p. End of use case.
q. Note: Violations must be inspected according to the code version that was in effect at the time the device was accepted or a component was altered. This means that the System must keep a record of all code reference documents ever used and all alteration dates so that the Inspector can link each violation to a particular version of a code reference document.

5. The Inspector performs an alteration inspection
   a. This use case is triggered when:
      1) A Device Maintenance Company uses the public interface to inform NCDOL that an alteration or repair has been completed and
      2) The Inspector is onsite to do the inspection.
   b. Remainder of this use case is the same as routine inspection WITH THE EXCEPTION THAT:
      1) A new certificate is always created and signed.
      2) The System prompts the Inspector to indicate if the alteration inspection was thorough enough that the next routine inspection need not take place for one year. If yes, Inspector notes this in the record.
      3) If the alteration inspection is related to an accident and the inspection passes, the investigator can indicate that the accident investigation is closed. In that case, the Inspector may tell the Local Contact that the device may be put back in operation.
   c. End of use case.
   d. Note: Inspection information for an alteration is tied to the code reference document in effect at the time the alteration permit was approved.
6. The Inspector performs a compliance inspection (follow-up to routine inspection where a violation was found)
   a. This use case is triggered when:
      1) The Owner uses the public interface to inform NCDOL that all violations cited have been corrected
      OR
      2) An abatement period is ended AND a compliance inspection was required
      OR
      3) A new violation unrelated to an accident is found during an investigation
      AND
      4) The Inspector is onsite for the inspection.
   b. The Inspector performs the inspection.
   c. The Inspector logs onto the System and selects the **Compliance Inspection** function.
   d. The System displays all compliance inspections due:
      1) The Inspector can select one of the compliance inspections listed or enter a **State ID#** for a device not listed.
   e. System displays device information and data from the ongoing routine inspection, including any previous compliance inspections.
   f. Inspector determines if the device is in compliance for each violation and enters data relevant to the inspection into the System (e.g. device is in compliance; new violations found).
   g. Inspector indicates that data entry is complete.
   h. System displays the record so that the Inspector can review it. Inspector may edit the content, save the record, save entered data for later completion or cancel.
      1) If the record is saved as complete, the Inspector prints an inspection report and gives it to the onsite customer contact (e.g. Device Maintenance Company representative).
      2) After completing and saving an inspection record, the Inspector can:
         d) Open the record for edit (e.g. to correct an error) and/or

e) Reprint the inspection report.

i. If the inspection passes:
   1) The Inspector indicates that the inspection is complete in the System.
   2) The System saves the record.
   3) The System sets device status to **Normal Operation**.

j. If one or more minor violations that triggered the abatement are not repaired, the Inspector notes this in the System and sets a new abatement date from 1 to 90 days from the current date (Inspector discretion).

k. If one or more serious violations that triggered the abatement are not repaired, the Inspector (Note: certificate may have been removed previously and shutdown order may have been issued):
   1) Notes the failure to fix the violation(s) in the report.
   2) Sets an abatement date 1 to 10 days from the date of the current inspection.
   3) If certificate had been removed earlier, a new certificate is not reissued.

l. In subsequent compliance inspections and when the certificate of operation has been removed:
   1) If the same violation has not been repaired during the next compliance inspection the Inspector calls their Supervisor who may allow another 1 to 10 days. Inspector notes that a final extension has been granted in the record. A new certificate is not reissued.
   2) If the repair is still not made after the final extension, Inspector stops inspections until they hear from the Owner or Owner Representative or 12 months have passed.

m. In subsequent compliance inspections and when the certificate of operation has NOT been removed:
   1) If the same violation has not been repaired during the next compliance inspection the Inspector calls their Supervisor who may allow another 1 to 10 days. Inspector notes that a final extension has been granted in the record.
   2) If the repair is still not made after the final extension, Inspector removes their certificate for non-compliance. Inspector prints a shutdown order and a compliance inspection report that cites reasons for shutdown. Inspector gives the report to Owner or Owner Representative and explains steps they must take to get the device back in operation.

n. End of use case.

7. Condemning a device
   a. This use case is triggered when an Owner has not repaired a device and 12 months have elapsed since the final extension.
   b. After 12 months of inactivity, the System alerts the Inspector of an inactive certificate of operation. The Inspector does an inspection. If the elevator is still not in operation:
      1) The Inspector selects the **Condemn Device** function.
      2) The System prompts for a **State ID#**.
      3) The Inspector enters the **State ID#**.
      4) The System displays the **Condemn Device** data entry screen.
      5) The Inspector indicates that the device is still out of operation and must be condemned.
      6) The System sets device status to **Condemned**.
      7) The System prints an inspection report that indicates that the elevator is condemned. The report includes a list of owner responsibilities and direction on how to properly land the elevator. This is given to the Owner or Owner Representative.

8) The System prompts the Inspector on each annual anniversary of the condemnation to return and see if the elevator has been landed. There is a fee for each inspection.
9) Once the elevator has been landed, the Inspector indicates this in the System. There is no fee for that inspection. System sets device status to **Landed**.
10) System alerts the Inspector every 3 years to inspect the landed elevator. There is no fee for these inspections.
11) If the Inspector finds that the device has been destroyed, the Inspector indicates this in the System and the System sets device status to **Destroyed**.

c. If the Owner wants to bring the device back into operation:
   1) They contract with an Elevator Company to determine what work is required.
   2) The Elevator Company submits an alteration inspection request.
   3) See alteration inspection use case above.
d. End of use case.

8. Plan to perform inspections

Inspectors must plan each day of work taking into account the types of inspection, whether or not routine inspections are overdue, location of device, start location of the Inspector and other parameters. The intent is to inspect as many devices as possible in a day. The vendor is expected to develop an algorithm to assist in this planning e.g. by displaying the most efficient route to travel among selected sites.

a. This use case is triggered when an Inspector needs to plan a day's work.
   1) Note: this function also takes amusement inspections into account.
b. The Inspector logs onto the System and selects the **Plan Inspections** function.
c. System lists all devices that require inspection.
   1) Devices are sorted by category as follows:
      a) New inspections
      b) Routine inspections
      c) Modification inspections
      d) Compliance inspections
      e) Amusement inspections
      f) Special (no inspection needed but a visit to the site is required for any of several reasons including lost certificate; new Local Contact requests new certificate, examine condemned device)
   2) For routine inspections, the devices are sorted in order of days overdue.
   3) When compliance inspections are needed they appear in the list 2 days before they are due or when the Owner has reported that the work has been completed.
   4) Data displayed for each device includes the code reference document that the device must comply with so Inspector knows which code reference document to use.
   5) Devices are flagged if they need to be taken out of operation (i.e. by removing certificate) due to non-payment, or if the 90-day certificate expires.
   6) Location of each device is shown.
d. Inspector selects the devices to inspect.
e. System determines most efficient route, considering Inspector starting point and other data, and provides the information to the Inspector.
f. Inspector can change device selection and see the impact on routing.
g. Inspector can save the list of inspections as final, close the list for completion later, or cancel.
h. Once the list is saved, the Inspector can download the information (e.g. in PDF or to a mobile device), print the list, open the list for edit or exit the function.
i. End of use case.

1) Note: When an Inspector uses this function data are limited to the Inspector's assigned set of devices.
2) Note: When a Supervisor uses this function, the Supervisor can see devices for all Inspectors in their region and can assign any device to any Inspector.
3) Note: When Management uses the function, they can see all devices for all Inspectors in all regions and can assign any device to any Inspector.

9. Inspector or Back Office enter a new incident or accident in the System

Inspectors also serve as investigators when there is an event that involves human injury or damage to a device. Some events are minor (i.e. incident) and some are major (i.e. accident). These events must be logged into the System.

a. This use case is triggered when an event is reported to the Back Office.
b. When an event occurs, someone (e.g. the Owner, Local Contact, Elevator Company or someone from the general public) calls it in by phone to the Back Office or Inspector.
c. User records event information into the System. Information includes for example:
    1) Name, phone number and email of person reporting the incident
    2) Time
    3) Building
    4) Describe incident
    5) Type of equipment
    6) Was this equipment failure or rider error?
    7) Was an ambulance required? If yes, this is an accident.
    8) Was first aid or less required? If yes, this is an incident.
    9) Other information as provided
d. System records date and time that the accident is reported.
e. By default the System records all events as an incident.
f. User can save the information, edit the information, save entered data for later completion or cancel.
g. Once data are saved, the System puts a notice in the My Communications section of the Supervisor and local Inspector in the region where the event occurred. The alert includes contact information of the person reporting the incident.
h. End of use case.

10. Inspector investigates an incident or accident

Inspectors also serve as investigators when there is an event that involves human injury or damage to a device. Some events are minor (i.e. incident) and some are major (i.e. accident). All events are investigated. All events must be logged into the System.

a. This use case is triggered when the System places notice of an event in the My Communications section of the Supervisor and local Inspector in the region where the event occurred.
b. Supervisor ensures that an Inspector is assigned to perform the inspection.
c. The investigator decides if the event was an:
    1) Incident (minor)
        a) Investigator generates a report:
            i. Investigator logs onto the System.
            ii. Investigator selects the **Incident Report** function.
            iii. System prompts for a **State ID#**.
            iv. Investigator enters a **State ID#**.
            v. System displays the **Incident Report** data entry screen pre-populated with available information.
            vi. Investigator enters incident data.
            vii. Investigator indicates that data entry is complete.

viii. System displays data for review.
ix. Investigator reviews data. Investigator can save data, save data for completion later, edit data or cancel.
1. When data are saved, System saves the information.

2) Accident (major)
a) Owner is required to prevent use of the device or else call the Maintenance Company to shut it down. They must contact the Bureau and report the accident.
b) Investigator goes to site within a day and investigates. Maintenance Company or other onsite representative provides information to the Investigator.
c) Investigator determines cause of accident.
d) Investigator logs onto the System and selects the **Accident Report** function.
e) System prompts for a **State ID#**.
f) Investigator enters a **State ID#**.
g) System displays an accident report screen pre-populated with available information.
h) Investigator enters an accident report into the System:
i. Investigator enters accident data.
ii. Investigator may take digital photos onsite and upload them into the System.
iii. Investigator indicates that data entry is complete.
iv. System displays data for review.
v. Investigator reviews data. Investigator can save data, save data for completion later, edit data or cancel.
1. When data are saved, System saves the information.
a) Investigator sends paper documents and physical evidence to the Back Office via US Post.
b) The Back Office Staff scan it all and store that via Filenet under the State ID# as part of the accident data.
c) Physical evidence may be stored. The System tracks anything that is stored.
a. PROCESS TO BE DEFINED

d. End of use case.
e. Note:
1) If a new violation unrelated to the accident is found during an investigation the investigator does a compliance inspection.
2) The System must assign a unique ID# to every incident and accident report.
3) If the investigator is present when repairs are done, no alteration permit is required for accident-related repairs.
4) If the repair will take time, then an alteration permit may be required. This is dictated by the violation code reference documents and the investigator enters what is required into the System.
5) When repair is required, the Owner or Owner representative has the Maintenance Company perform the repair.
6) Maintenance Company uses the public interface to indicate that the repair is done when that is required (Inspector discretion).
a. When the Maintenance Company reports that the repair is done via the public interface, the System creates a flag for an accident follow-up compliance inspection. Notice is put in the My Communications section of the Inspector.

7) When a follow-up compliance inspection is required, the Inspector enters inspection results into the device record as a compliance inspection report. The System indicates that the compliance inspection is related to an accident.
8) If the Inspector finds the repair to be satisfactory, the Inspector informs the Owner or Owner representative that they may put the device back into operation.
9) If the repair is inadequate:
    a. The Inspector informs the Owner or Owner representative that repair must be completed satisfactorily before the device can be used again.
10) All accident information becomes available to the general public.

11. Inspector fills out a daily work report
    a. This use case is triggered when an Inspector needs to report details of a day's work. Data are entered by the Inspector.
    b. Inspector logs onto the System and selects the **Daily Work Report** function.
    c. System displays the **Daily Work Report** data entry screen.
    d. Inspector enters daily report data including:
        1) Production for the day, e.g. time driving, mileage, time in field, conference time (i.e. time spent with Owner where no fee is levied); holiday, comp, etc.
        2) Miles travelled are tracked separately for elevator inspections versus amusement inspections.
        3) System must prompt Inspector for morning and evening odometer reading, start and end time, etc.
        4) As needed, the Inspector can use System prompts to print:
            a. Daily results on State Mileage log form to Motor Fleet
            b. Monthly mileage report
            c. Monthly expense report
    e. Inspector indicates that data entry is complete.
    f. System displays the record so that the Inspector can review it. Inspector may edit the content, save the record, save entered data for later completion or cancel.
        1) If the record is saved as complete, the Inspector can print a copy or save in electronic form (e.g. PDF).
        2) After completing and saving the record, the Inspector can:
            a. Open the record for edit (e.g. to correct an error) and/or
            b. Reprint the record.
    g. End of use case.
12. Inspector edits device information
    a. This use case is triggered when an Inspector finds it necessary to modify information in a device record.
        1) When the Elevator System is designed, specific fields that Inspectors can and cannot update must be determined by vendor with detailed CRUD analysis (e.g. Inspectors cannot update State ID#, install date, original test date).
    b. Inspector logs onto the System and selects the function.
    c. System prompts for search criteria.
    d. Inspector searches for the device, e.g. enters the State ID#, Owner, etc.
    e. System displays a list of various aspects of the record, e.g. device descriptive data (device type), inspection data, investigation data, addresses, etc.
    f. Inspector chooses type of information to change.
    g. System allows Inspector to drill down to the level of detail required.
    h. Investigator makes the changes.
    i. Inspector indicates that data entry is complete.
    j. System displays the changes and requests confirmation.
    k. Inspector confirms the change.

l. Inspector may edit the content, save the record, save entered data for later completion or cancel.
m. End of use case.

13. Inspector changes contact information for all devices at an address
    a. This use case is triggered when an Inspector needs to change an address associated with one or more devices.
    b. User selects function.
    c. System prompts for an address.
    d. User enters an address.
    e. System displays a list of all matches.
    f. User selects an address.
    g. System displays a list of all devices located at that address.
    h. User selects each device affected by the contact information change (or **Select All**).
    i. User selects the type of address to change.
    j. User enters new data.
    k. User indicates that data entry is complete.
    l. System displays all changes.
    m. User reviews data and can accept, edit or cancel.
    n. End of use case.
14. Inspector views the Inspector Library

    The Inspector Library is a collection of reference documents that are used routinely by Inspectors in the field.

    a. The following are possible features of the library:
        1) An index of all library contents
        2) All files in PDF
        3) A search system
        4) Can select and print specific text, or print the whole document
    b. This use case is triggered when an Inspector or other authorized person wants to read the contents of an inspection guide or code book.
    c. Inspector logs onto the System and selects the function.
    d. System displays an index of available documents.
    e. Investigator selects a document.
    f. System displays the document.
    g. Investigator views the document.
    h. Investigator can close the document and return to index of library contents or exit the function.
    i. End of use case.

B. Customers

These use cases assume that the Customer has Internet access. However, the System must allow the Back Office to perform any function for a Customer who does not have access to the public interface. This may include having the Back Office Staff accept information via phone, mailing paper forms to the Customer to fill out, etc. Also, the System must have a means of protecting the public interface from robotic entry of garbage data, e.g. by having Users at login enter text that is displayed in graphic format.

1. Customer applies for new device permit
    a. This use case is triggered when a device company (e.g. an Elevator Company) needs a permit to install a new device.

b. Permit request is entered by an authorized entity, e.g. the Elevator Company that will do the install, via public interface. Elevator Company Staff may request ID, password and PIN from Back Office online or by calling the Back Office Staff.
c. Authorized User enters ID and password to gain access to the public interface.
d. The User enters all data required for the permit request, e.g. equipment type, capacity, floor to floor landings, speed, volts, watts, code edition, location.
e. User uploads any required drawings.
f. User indicates request for standard or 90-day certificate.
g. [Future] User may select to pay application fee in advance. If they choose this, they can choose to:
    1) Pay via credit card.
    2) Request an invoice. In that case the System sends a notice to the My Communications section of Budget and they send an invoice to the Customer.
    3) Follow directions shown on screen to contact Budget for alternative payment methods (e.g. ACH).
h. User indicates completion of data entry.
i. The System stores the data.
j. System displays a summary of the request.
k. User reviews the data and has the option to:
    1) Edit the request.
    2) Submit the request.
    3) Cancel the request and return to menu.
l. Once the User submits the request, they can print the record, download the record (e.g. to PDF file), enter another permit, choose another function or exit the System.
m. If the request is for a standard certificate, the System puts an alert in the My Communications section of the Engineer's workplace.
n. If the request is for a 90-day certificate, the request is forwarded to the My Communications section of the relevant Inspector and their Supervisor. It is up to the Customer to initiate further action by the Inspector (e.g. via phone call).
o. End of use case.

2. Customer applies for a permit that allows modification of a device
    a. This use case is triggered when an authorized User needs a permit to alter or repair a device. On the public interface, the permit request must be entered by an authorized entity, i.e. Device Maintenance Company.
    b. Authorized User enters ID and password to gain access to the public interface.
    c. User enters **State ID#**.
    d. System displays data for the relevant device.
    e. User enters all data required for the permit request, e.g. modification type (i.e. alteration or repair), description of work.
    f. User indicates completion of data entry.
    g. System displays a summary of the request.
    h. User reviews the data and has the option to::
        1) Edit the request.
        2) Submit the request. The System stores the data and flags the record as **Available for Review**. System forwards the request to the Engineer for approval.
        3) Cancel the request and return to menu.
    i. Once the User submits the request, they can print the record, download the record (e.g. to PDF file), enter another permit, choose another function or exit the System.
    j. End of use case.
    k. Note: System will allow any number of modification requests. A request may be made even if prior requests are not yet approved or work completed.

3. Customer reports work completed
    a. This use case is triggered when an authorized party needs to report that installation of a new device is complete.
    b. Report is entered by an authorized person, e.g. Elevator Company, Device Maintenance Company, etc. via public interface.
    c. Authorized User enters ID and password to gain access to the public interface.
    d. User chooses the function.
    e. System prompts for **State ID#** of the device.
    f. User enters the **State ID#** .
    g. System displays data entry screen.
    h. User indicates that the work is for one of the following:
        1) New installation
        2) Modification
        3) Compliance
    i. User indicates that new installation work has been completed.
    j. User indicates completion of data entry.
    k. System displays a summary of the request.
    l. User reviews the data and has the option to:
        1) Edit the request.
        2) Submit the request. The System stores the data and forwards a request for inspection to the assigned Inspector's My Communication section.
        3) Cancel the request and return to menu.
    m. Once the User submits the request, they can print the record, download the record (e.g. to PDF file), report installation work completed on another device, choose another function or exit the System.
    n. End of use case.
4. Customer requests a variance
    a. This use case is triggered when a General Contractor of Record or Elevator Company cannot meet code and therefore requires a variance.
    b. Authorized User, e.g. Installer, enters ID and password to gain access to the public interface.
    c. User selects the function.
    d. System prompts for **State ID#** of the device.
    e. User enters the **State ID#** .
    f. System displays data entry screen.
    g. User enters the specific code(s) that the variance(s) will apply to.
    h. User enters an explanation of what variance is needed and why.
    i. User uploads scans of drawings and photos as needed.
    j. User indicates completion of data entry.
    k. System displays a summary of the request.
    l. User reviews the data and has the option to:
        1) Edit the request.
        2) Submit the request. The System stores the data.
        3) Cancel the request and return to menu.
    m. Once the User submits the request, they can print the record, download the record (e.g. to PDF file), request another variance, choose another function or exit the System.
    n. Once data are submitted, System forwards the request to the My Communications section of the Bureau Chief.
    o. End of use case.

5. Customer requests a replacement certificate
    a. This use case is triggered when an Owner or Owner representative needs a replacement certificate, e.g. to replace a certificate that has been lost from one of their device(s) (e.g. through theft, vandalism, accident, etc) or because there is a new Owner.
    b. Authorized User (e.g. Owner or Owner Proxy) enters ID and password to gain access to the public interface.
    c. User selects the function.
    d. System prompts for **State ID#** of the device.
    e. User enters the **State ID#**.
    f. If there is no reason not to print a certificate, then the System will provide a PDF file for the User to download and print. Signatures on the certificate (i.e. Commissioner, Bureau Chief and last Inspector) are digital facsimiles.
    g. Once the User submits the request, they can print the certificate, download the file (e.g. to PDF file), request another replacement certificate, choose another function or exit the System.
    h. End of use case.
6. Customer requests to place certificate in a location other than the elevator
    a. This use case is triggered when an Owner or Owner representative wants to place the certificate in a safe place, e.g. when there is concern about theft, vandalism, etc).
    b. Authorized User (e.g. Owner or Owner Proxy) enters ID and password to gain access to the public interface.
    c. User selects the function.
    d. System prompts for **State ID#** of the device.
    e. User enters the **State ID#**.
    f. System displays data entry screen.
    g. User explains the request.
    h. User indicates completion of data entry.
    i. System displays a summary of the request.
    j. User reviews the data and has the option to:
        1) Edit the request.
        2) Submit the request. The System stores the data and flags the record as **Available for Review**. System also submits the request to the My Communications section of the Bureau Chief.
        3) Cancel the request and return to menu.
    k. Once the User submits the request, they can print the record, download the record (e.g. to PDF file), request another certificate, choose another function or exit the System.
    l. End of use case.
7. Customer obtains information about their devices
    a. This use case is triggered when a Customer wants to obtain information about their device(s) from the public interface.
    b. Customer enters ID and password to gain access to the public interface.
    c. Customer can select from any of a number of reports shown, such as:
        1) Obtain inspection report
        2) Inspection history (list of inspections with detail available)
        3) Invoice history (list of invoices with detail available)
        4) Violations history (list of violations with detail available)
        5) Investigations history (list of investigations with detail available)
    d. In all cases:
        1) Customer enters **State ID#** of device or other identifying information as search criteria.
        2) System displays a list of devices that match search criteria and that are related to Customer.

g) System tracks devices to which each Customer has a relationship. For example, System will only display to Owner devices that they own, to Maintenance Company devices for which they have a contract, etc.
3) Customer selects device.
4) System displays relevant data.
5) Customer has the option of viewing, printing and downloading (e.g. to PDF format) the information.
6) Customer may return to menu or exit function.

e. End of use case.

8. Customer (e.g. new Owner, new Local Contact, Installer) submits request to obtain ID and password for the public system
    a. This use case is triggered when a new Customer needs to obtain a user ID and password to use on the public interface.
    b. Customer navigates to the public interface and selects the function.
    c. System displays a list of roles (e.g. Owner, Elevator Company, Maintenance Company).
    d. User selects all roles that they fill.
    e. System presents a screen that requests data specific to the role(s).
    f. User fills in the data.
    g. User reviews the data.
    h. User may submit the request, edit the data or cancel.
    i. If User submits the request:
        1) System puts information into temporary storage pending review by Back Office.
        2) System puts an alert in the My Communications section of the Back Office that a user ID request is pending their review.
    j. User may do any of the following: print the data, download the data (e.g. to PDF file), exit the function.
    k. End of use case.
9. Customer maintains their ID and password in public system
    a. This use case is triggered when a Customer wants to change their user ID and/or password on the public interface.
    b. Customer enters ID and password to gain access to the public interface.
    c. Customer selects the function.
    d. System uses Bureau standard procedure to change ID and/or password.
    e. System supports use of security questions.
    f. System supports sending temporary ID and/or password to email address of record.
    g. When done, User exits System to obtain new ID and or password.
    h. End of use case.
    i. Note: The Back Office can do this function for the Customer. If Customer calls Back Office and requests it, Back Office User can have System send a new ID and or password to the Customer.
        1) To be determined: this function may tie into the Bureau's uniform logon infrastructure. It may be NCID driven.
10. Customer pays invoice
    a. This use case is triggered when the Customer wants to pay an invoice online.
    b. Customer (User) logs onto public interface with valid ID and password.
    c. User selects function.
    d. System displays list of unpaid invoices.
    e. User selects invoice.
    f. System displays invoice.
    g. User can pay invoice, print invoice, return to menu. If User wants to pay the invoice:
        1) User indicates a desire to pay the invoice.
        2) System presents payment options.

3) User selects option and pays invoice.
4) System confirms payment.
5) User can print payment confirmation.

h. Once the Customer completes payment they can choose another invoice, another function or exit the System.
i. End of use case.

C. Back Office

System functions specifically performed by the Back Office include the following.

1. Engineer reviews a new device permit request – standard certificate
    a. This use case is triggered when a device manufacturer (e.g. Elevator Company) applies for a permit to install a new device (e.g. elevator, escalator), and the Engineer checks My Communications and discovers that there is a new permit application.
    b. Engineer opens the application for a new permit.
    c. System displays the data.
    d. The Engineer reviews the application data:
        1) If the data are non-valid (e.g. spam) the Engineer deletes the application from the System. The System challenges the deletion with "Are you sure?" After deletion the System maintains no record of this action. Engineer also alerts Back Office that the ID and password may be compromised.
        2) If the Engineer approves the application, the System.
            a) Assigns a **State ID#** to the device described in the request.
            b) Assigns an Inspector to the device.
            c) Creates a permit that allows the construction company to proceed with the work (PDF file).
            d) Creates a completed application form that shows it approved (PDF file).
            e) When an email address is available, the System emails the PDF files to the applicant. Email content is predefined and includes instructions for the applicant and the name and contact information of the assigned Inspector. It is up to the Customer to contact the Inspector for the first inspection.
                a. When no email address is available, the Engineer can print the documents and mail them via US Post to the applicant.
        3) If the Engineer does not approve the application:
            a) When an email address is available, the System emails a rejection notice to the applicant that includes the reason for rejection as entered into the System by the Engineer. The notice includes the Engineer's contact information. It is up to the Customer to contact the Engineer for further action.
                b. If an email address is not available, the Engineer can print the notice and mail it via US Post to the Customer.
            b) When the Customer contacts the Engineer, the Engineer works out the details until all criteria for the application are met, notes all decisions and actions in the record, and then goes through the approval process described above.
    e. End of use case.
2. Back Office acts on a possibly compromised Customer ID and password
    a. This use case is triggered when anyone in the Back Office receives a bogus request through the public interface and an ID and password would have been required to enter it.
    b. Back Office Staff suspend ID from further use.
    c. Back Office Staff contacts IT Staff and reports the problem.
    d. Further actions to be determined during the business process reengineering.

3. Review a modification permit request
    a. This use case is triggered when a Device Maintenance Company applies for a permit to alter or repair a device (e.g. elevator, escalator).

       Modification permits include two work types, alteration (major changes) and repairs (minor work). The distinction is important because the code used in the System is different between the two. It is important that the work type is consistent with the description of the work to be done, and this is determined by the Engineer.

    b. The Engineer checks My Communications and discovers that there is a modification permit application.
    c. The Engineer reviews the application data:
        1) If the data are non-valid (e.g. spam) the Engineer deletes the application from the System. The System challenges the deletion with "Are you sure?" After deletion the System maintains no record of this action. The Engineer also alerts the Back Office that the ID and password may be compromised.
        2) If the Engineer approves the application, the System:
            a) Creates a permit that allows the Device Maintenance Company to proceed with the work (PDF file).
            b) Creates a completed application (PDF file).
            c) If an email address is available, the System emails the PDF files to the applicant. Email content is predefined and includes instructions for the applicant.
                c. If no email address is available, the Engineer can print the documents and mail them via US Post to the applicant.
        3) If the Engineer does not approve the application:
            a) When an email address is available, the System emails a rejection notice to the applicant that includes the reason for rejection as entered into the System by the Engineer. The notice includes the Engineer's contact information. It is up to the Customer to contact the Engineer for further action.
                d. If an email address is not available, the Engineer can print the notice and mail it via US Post to the Customer.
            b) When the Customer contacts the Engineer, the Engineer works out the details until all criteria for the application are met, notes all decisions and actions in the record, and then goes through the approval process described above.
    d. The approved application document contains the name and contact information of the assigned Inspector so that the applicant can contact the Inspector for an inspection.
    e. End of use case.
4. Send a revocation letter
    a. This use case is used on a weekly basis.
    b. At least once each week, an authorized User in the Back Office runs a late payment function.
    c. System displays a list of all payments more than 90 days late.
    d. User reviews records and indicates any that should be deferred or cancelled.
    e. For all selected invoices the User can have the System create a notice of revocation letter (e.g. PDF file) from the Bureau Chief threatening loss of operating certificate if the invoice is not paid within 30 days. In addition, the User can have the System create a copy of the invoice with "Final Notice" added (e.g. PDF file).
    f. User indicates completion of data entry.
    g. System displays a summary of the data.
    h. User reviews the data and has the option to:
        1) Edit the data.

2) Submit the data.
3) Cancel the request and return to menu.

i. System saves a submitted request.
j. System generates the letters and places them in the appropriate Inspector's My Communications section of the application for their information; no action is required on the Inspector's part.
k. System prints the letters and Back Office Staff mails them to the billing address.
l. In addition, the System puts a copy of the revocation letter in the My Communications section as follows:
    1) If it is for an Elevator Company or Maintenance Company it goes to the Bureau Chief.
    2) If it is for anyone else it goes to Budget.
m. If, after 30 days, the Customer has not paid the invoice the System alerts the Inspector to remove the device certificate through notice in their My Communications section. The Supervisor and Bureau Chief are also notified that this action has been initiated. The Inspector enters into the device record the date on which the certificate was removed.
n. When the Owner pays the bill and wants to put the device back into operation they must request a compliance inspection. There is no fee for this inspection.
o. End of use case.

5. Back Office edits address/contact information
    a. This use case is triggered when a Customer address and or other contact information has changed.
    b. Back Office User logs onto System and selects function.
    c. System gives User choice of changing address as follows:
        1) By device
        2) Address of a specific Owner, Property Management Company, etc.
        3) Mass address change
    d. For device level:
        1) System prompts for **State ID#**.
        2) User enters number.
        3) System displays all addresses for that device.
        4) User enters new address information.
        5) System requests confirmation.
        6) User can confirm, edit or cancel.
        7) If confirmed, System saves data.
        8) Note: Back Office can enter a new billing address but this must be verified by Budget before it becomes permanent in the System.
    e. At property level to change contact information for all devices at that address:
        1) System prompts for an address.
        2) User enters an address.
        3) System displays a list of all matches.
        4) User selects an address.
        5) System displays a list of all devices located at that address.
        6) User selects all devices affected by the contact information change.
        7) User selects the type of address to change.
        8) User enters new data.
        9) User indicates that data entry is complete.
        10) System displays all changes.
        11) User reviews data and can accept, edit or cancel.
    f. For Owner, Property Management Company, etc.
        1) System prompts for identifying name.
        2) User enters name.

3) System displays matching hits.
4) User selects from the list.
5) System displays relevant data.
6) User updates data.
7) System requests confirmation.
8) User can confirm, edit or cancel.
9) If confirmed, System saves data.

g. For mass change:
   1) User searches for records (e.g. all J.C.Penney stores).
   2) System displays all records that meet the search criteria.
   3) User selects address type to change (i.e. Owner, Billing, Property Management Company, Maintenance Company).
   4) User selects records to change.
   5) System prompts for the new address.
   6) User enters new address.
   7) System requests confirmation of address change.
   8) User can confirm, edit address or cancel.
   9) If User confirms address change, System changes the address in all selected records.
h. End of use case.
i. Note: this function cannot be used to change the Owner, Elevator Company etc. within an inspection record. Rather it only replaces their address in all open and active records and in all future work.
j. In the legacy System there are four unique addresses. However, there appear actually to be eight unique addresses for each device: There can be defaults in the System that eliminate double data entry.
k. Address types are:
   1) **Applicant** (usually the Elevator Company). By default this is also the initial Billing Address.
   2) **Owner** – the entity that actually owns the building where the device is located. The State ID# belongs to the Owner. Owner is ultimately responsible for their devices. Some Owners are difficult to communicate with. Some do not want to be directly involved and so work through a Property Management Company (see below). Owners may be out of state or even out of the country. A building may be in foreclosure with the Owner unclear.
      - Note: It is necessary to accept postal codes, phone number format etc for foreign countries. Country will be USA and state will be North Carolina by default.
   3) **Local Contact** – the entity that is responsible for day to day operations of the building where the device is located. Usually the Local Contact resides in or has an office in the building, but it is possible that Local Contact is in one of several related buildings, in which case several physical addresses could share the same Local Contact. There can be multiple Local Contacts for a single device.
   4) **Physical** – actual street address where the device is located.
   5) **Billing** – the entity responsible for paying fees and fines. Bills can be paid by the Applicant, Owner, Local Contact, Maintenance Company or Property Management Company.
   6) **Maintenance** – the company that is responsible for maintenance of the device. Used by Budget for invoicing new and alteration invoices. By default this is the Elevator Company who did the install but it can be changed.
   7) **Property Management Company** – an optional entity that may serve as proxy for the Owner and/or Local Contact.

8) **General Contractor** – e.g. a company that hires the Elevator Company to install an elevator.

l. Relationships among addresses are complex. The following are shown here as an example; many other relationships exist:
   1) An Owner can have none or many Property Management Companies.
   2) An Owner can have one or many Local Contacts.
   3) A Local Contact has one Owner.
   4) A Local Contact may work through none or one Property Management Company.
   5) A Property Management Company may work with one or many Owners.
   6) A Property Management Company may work with one or many Local Contacts.

m. The System should make it easy to copy any address into another address, e.g. it should be easy to copy the physical address into the Local Contact address.

6. Back Office performs customer functions for a Customer
   a. This use case is triggered when a Customer cannot access the public interface and needs to submit a request, supply information, etc. The Back Office Staff can perform any customer function. In each case:
      1) Local Contact calls the Back Office Staff and explains what they need.
      2) Back Office Staff confirm identity of caller.
      3) Back Office Staff performs the function.
      4) The System gives the Back Office Staff a confirmation number which they provide to the Customer.
      5) The System performs all usual actions associated with the specific function.
      6) Back Office Staff saves the record and has the option of printing the request or exiting the function.
   b. End of use case.
7. Back Office Staff manages fees and fines
   a. This use case is triggered when there is need to change, remove or create a fee or a fine.
   b. User selects the function **Manage Fees** or **Manage Fines**. Both work the same way.
   c. System presents options of **Modify**, **Delete** or **Create Fee/Fine**.
   d. User selects an option.
   e. For **Modify:**
      1) System presents a list of currently used fees/fines.
      2) User selects a fee/fine.
      3) System presents fee/fine data.
      4) User can modify name of fee or amount of fee/fine.
      5) User enters date on which the changed fee/fine becomes active.
      6) User can:
         a. Save data:
            i. System saves data to database.
            ii. System keeps history when data are changed.
            iii. Changed fee/fine is available as of the activation date for all new transactions, but existing transactions are not changed.
         b. Return to menu.
   f. For **Delete:**
      1) System presents a list of currently used fees/fines.
      2) User selects a fee/fine.
      3) System presents fee/fine data and requests confirmation to delete.
      4) User can:
         a. Confirm deletion:

i. System saves changes to database.
ii. Deleted fee/fine no longer appears in any relevant dropdown and in all future relevant internal calculations its value is zero.
iii. Deleted fee/fine is kept in all current (active) records where it has already been selected.
iv. System keeps history.

b. Return to menu.

g. For **Create:**
1) System presents a data entry screen.
2) User enters data related to the new fee/fine (e.g. name of fee/fine, amount of fee/fine, activation date).
3) System presents fee/fine data and requests confirmation to create.
4) User reviews new fee/fine data. User can:
a. Save new fee/fine:
i. System saves changes to database.
ii. As of the activation date the new fee/fine appears in any relevant dropdown and its value is included in all relevant internal calculations.
b. Cancel and return to menu.

h. System maintains a record of actual fee or fine levied with each transaction, i.e. the same device may have a record of different fees charged for the same inspection at different times.
i. End of use case.
j. Note:
1) It must be possible to include any new fee/fine or fine in a relevant invoice.
2) It must be possible to include any new fee/fine or fine in an inspection.

8. Back Office creates a new equipment type
a. This use case is triggered when a manufacturer introduces a new kind of equipment on the market and requests permission to install one for the first time.
b. Equipment has multiple attributes such as:
1) Name
2) Description
3) Code book
4) Version of code book
5) Drive type (e.g. rope, chain, hydraulic)
6) Fee (e.g. dumb waiter and handicap routine inspection fee is $65)
c. User selects function.
d. System prompts for equipment type data.
e. User enters equipment type data.
f. User indicates that data entry is complete.
g. System displays data for review.
h. User reviews data. User can save, edit, save entered data for later completion or cancel.
i. When data are saved, System adds the new equipment to the System.
j. End of use case.

9. Back Office creates a new operation type
a. This use case is triggered when a manufacturer introduces a new kind of operation type on the market and requests permission to install one for the first time.
b. Operation types have multiple attributes including:
1) Name
2) Description
c. User selects function.

d. System prompts for operation type data.
e. User enters operation type data.
f. User indicates that data entry is complete.
g. System displays data for review.
h. User reviews data. User can save, edit, save entered data for later completion or cancel.
i. When data are saved, System adds the new operation type to the System.
j. End of use case.

10. Authorized User (e.g. Back Office, Inspector) edits equipment data
    a. This use case is triggered when it is necessary to edit the data of a specific installed piece of equipment (e.g. to correct an error in data entry about a specific elevator).
        1) Note: addresses are considered in a separate use case.
    b. Authorized User logs onto System and selects function.
    c. System prompts for search criteria.
    d. User enters a **State ID#** or searches for and finds the appropriate equipment record.
    e. User modifies data permitted at their level of access.
        1) As part of the Elevator System implementation project, the vendor will determine details of what data each role can access via CRUD analysis or similar technique.
    f. User indicates completion of data entry.
    g. System displays a summary of the request.
    h. User reviews the data and has the option to:
        1) Submit the request:
            i. System saves a submitted request.
            ii. System keeps a record of old data.
        2) Edit the request.
        3) Save entered data for later completion.
        4) Cancel the request and return to menu.
    i. End of use case.
11. Back Office works with dropdown lists
    a. This use case is triggered when there is need to add or retire an item from a dropdown list. All dropdown lists in the System (except those maintained by Budget) can be maintained through this function. Dropdown lists include equipment type, operation type, etc. Note: violation codes are handled separately.
    b. User logs onto the System and selects the function.
    c. System displays a menu of dropdown lists.
    d. User chooses a dropdown list.
    e. User chooses from **Add to List**, **Archive Item**, **Un-Archive Item**
        1) **Add to List**: User enters the new item and selects **Save**.
        2) **Archive Item**: User chooses the item from the list and selects **Archive**. System marks this item with status **Archived**. Archived dropdown list items do not appear in any future use of the System (except this one) but are maintained in the System for prior records.
        3) **Un-Archive Item**: User chooses the item from the list and selects **Un-Archive**. System marks this item with status **Active**. Active dropdown list items appear in all future uses of the System.
    f. User indicates completion of data entry.
    g. System displays a summary of the changes.
    h. User reviews the changes and has the option to:
        1) Submit the request:
            i. System saves a submitted request.
            ii. System keeps a record of old data.
        2) Edit the request.

3) Save entered data for later completion.
4) Cancel the request and return to menu.

i. End of use case.

12. Authorized User (e.g. Back Office, Bureau Chief) creates a new Inspector or Supervisor
    a. This use case is triggered when a new Inspector or Supervisor is named.
    b. User logs onto the System and selects the function.
    c. System displays the **Create New Inspector / Supervisor** screen.
    d. User enters all information needed to define a new Inspector, including for example:
        1) Name
        2) Supervisor
        3) Home address
        4) Contact information
        5) Inspector ID#
    e. If the new person is a Supervisor, the User indicates this in the System.
    f. User indicates completion of data entry.
    g. System displays a summary of the changes.
    h. User reviews the changes and has the option to:
        1) Submit the request:
            a) System saves a submitted request.
        2) Edit the request.
        3) Save entered data for later completion.
        4) Cancel the request and return to menu.
    i. End of use case.
    j. Note: A new Inspector may add to the total number of Inspectors or replace an Inspector. In this case use the **Define Inspector Territory** function to reassign devices taking into account the location of the new Inspector.
    k. Note: A new Supervisor may add to the total number of Supervisors in the Bureau or replace an existing one. The User manually reassigns Inspectors to Supervisors.
13. Authorized User (e.g. Back Office, Bureau Chief) edits Inspector or Supervisor
    a. This use case is triggered when data associated with an Inspector must be changed.
    b. User logs onto the System and selects the function.
    c. System displays a list of Inspectors and Supervisors.
    d. User selects one person from the list.
    e. System displays that person's data for edit.
    f. User enters all information needed to update the record.
    g. User indicates completion of data entry.
    h. System displays a summary of the changes.
    i. User reviews the changes and has the option to:
        1) Submit the request:
            a) System saves a submitted request.
        2) Edit the request.
        3) Cancel the request and return to menu.
    j. End of use case.
14. Authorized User (e.g. Back Office, Bureau Chief) changes Inspector assignments to Supervisor
    a. This use case is triggered when it is necessary to assign an Inspector to a Supervisor, as when a new Inspector is hired or when an Inspector is moved from one Supervisor to another. It allows an Authorized User to manually reassign an Inspector to a different Supervisor.
    b. User logs onto the System and selects the function.
    c. System displays a list of Supervisors.
    d. User selects a Supervisor.

e. System displays a list of all Inspectors and indicates those who do not report to the selected Supervisor.
f. User can select one or more Inspectors to add to the Supervisor.
g. User can select one or more Inspectors to remove from the Supervisor.
h. User indicates completion of data entry.
i. System displays a summary of the changes.
j. User reviews the changes and has the option to:
    1) Submit the request:
        a) System saves a submitted request.
    2) Edit the request.
    3) Save entered data for later completion.
    4) Cancel the request and return to menu.
k. End of use case.
l. Note: The System transfers all functions relative to the moved Inspector to their new Supervisor, e.g. all System alerts that had been sent to the old Supervisor and not yet acted on are placed in the My Communications section of the new Supervisor.

15. Back Office performs an automated System function
    a. This use case is triggered when Back Office Staff have a need to perform a function that is normally done automatically by the System, e.g. when that function failed to run, ran improperly or when output from a run was lost.
    b. End of use case.
16. Back Office sends a penalty letter
    a. This use case is triggered when there is need to send a penalty letter.
    b. Authorized User logs onto the System and selects the function.
    c. System displays a list of devices with penalty that require a letter.
    d. User selects which letter should be sent, deferred or cancelled.
    e. User indicates completion of data entry.
    f. System displays a summary of who will get letters.
    g. User reviews the changes and has the option to:
        1) Edit the request.
        2) Submit the request.
        3) Cancel the request and return to menu.
    h. System saves a submitted request.
    i. System prints letters as directed.
    j. User mails letters certified return receipt requested.
    k. User enters date that letter was sent.
    l. User can choose another function or exit the System.
    m. End of use case.
17. Back Office enters certified mail green card data
    a. This use case is triggered when Back Office receives a Proof of Service from the USPS, which a Customer signs after receiving a penalty letter. This Proof of Service is commonly referred to as a “green card,” because of the color of the receipt issued by the USPS.
    b. Authorized User logs onto the System and selects the function.
    c. System displays a list of all records where a green card is due.
    d. User selects all records where green card has been received.
    e. User indicates completion of data entry.
    f. System displays a summary of the data.
    g. User reviews the data and has the option to:
        1) Edit the data.
        2) Submit the data.
        3) Cancel the request and return to menu.

h. System saves a submitted request and records the date that the card was received in each record.
i. User can choose another function or exit the System.
j. End of use case.

18. Back Office manages violation codes
    a. This use case is triggered when there is need to update the list of violation codes or create a new list.
    b. Violation codes come from multiple sources (e.g. ASME updated every 3 years; NFPA and ANSI updated at random times). In many cases (e.g. ANSI buck hoists and special equipment) Inspectors must cite violations according to the document. Codes come in both PDF and paper formats. It may be possible to scan paper documents if copyright issues can be cleared.
    c. There are over 2000 violation codes. It is not deemed feasible to hand enter all of the codes into the System every time there is an update. Options:
        1) Enter the most commonly encountered codes into the System for display in a dropdown list.
        2) Inspectors can add new codes to the dropdown list as they are encountered.
        3) Back Office updates dropdown lists whenever there is an update to a codes document.
        4) System keeps a history of all dropdown lists; violations must link to the code version that was in effect at the time of the violation.
        5) All versions of code books are maintained in the Inspector Library.
    d. Use case:
        1) Back Office User logs into the System and selects the function.
        2) System displays a menu of dropdown lists, with each list corresponding to a code set.
        3) User selects a dropdown list.
        4) User has the option of **Modify Dropdown List** or **Create New Dropdown List**.
        5) **Modify Dropdown List**:
            a) User can edit, create or delete an entry in the list.
            b) System will not allow deletion of an entry that is linked to a violation.
            c) User can change the document (in the Inspector Library) that the drop list is linked to.
            d) User can save the revised drop list or return to menu. When saved the revised list immediately becomes available to all Inspectors.
        6) **Create New Dropdown List**:
            a) User can create a new dropdown list and enter (manually or from electronic file) all code entries for the list.
            b) User must link the new dropdown list to a document in the Inspector Library.
            c) User can review the new list and correct entries.
            d) User can save the new dropdown list or return to menu. When saved the new list immediately becomes available to all Inspectors.
            e) System automatically archives the old list.
        7) Note: There is a dropdown list for each code document.
        8) If one or a few items in the list change, the System must track prior versions of those items. This is no need to have multiple versions of the same code list in its entirety.
    e. End of use case.

19. Back Office maintains the Inspector Library
    a. This use case is triggered when a new code book, inspection guide or other electronic document becomes available and there is need to make it available to Inspectors.
    b. Authorized User logs onto the System and selects the function.

c. System prompts for **Create**, **Modify** or **Delete a Document**.
d. **Create**:
    1) User enters the name of the document.
    2) User imports the document.
    3) User tests the new entry.
    4) User can Save the new entry (and System saves the data) or return to menu.
e. **Modify**:
    1) User selects the entry to modify.
    2) User edits the document name or uploads a replacement document.
    3) User test the revised entry.
    4) User can Save the new entry (and System saves the data) or return to menu.
f. **Delete**:
    1) User selects the entry to delete.
    2) System requests confirmation to delete (System will not allow a document that is linked to a code set to be deleted).
    3) User can confirm deletion (and System deletes document) or return to menu.
g. End of use case.

20. Back Office validates new Customer
    a. This use case is triggered when a new Customer has requested an ID and password so that they can use the public interface.
    b. Authorized User logs onto the System and selects the function.
    c. System displays a list of all requests for user ID and password.
    d. User selects each request one at a time.
    e. For each request:
        1) User reviews data.
        2) User verifies data as needed (e.g. phones the requestor).
        3) User updates data as needed.
        4) User indicates completion of data entry.
        5) System displays a summary of the data.
        6) User reviews the data and has the option to:
            a) Edit the data.
            b) Submit the request.
            c) Cancel the request and return to the list.
        7) System saves a submitted request.
        8) System assigns a temporary ID and password to the requestor.
        9) System assigns a unique ID# to each Customer (i.e. any customer type that might be billed such as Owner and Maintenance Company).
        10) System emails the logon information to the Customer.
    f. System displays the next request.
    g. User can review the next request, choose a different request, choose another function or exit the System.
    h. End of use case.
    i. Note: on first logon, new Customers are asked to change their ID and password.

21. Back Office creates/edits Customer
    a. This use case is triggered when there is need to enter a new Customer into the System or change customer data e.g. because the Customer cannot do it themselves. A Customer is anyone who might be billed and could, for example be any of the following:
        1) Owner
        2) Local Contact
        3) Elevator Company
        4) Maintenance Company
        5) Property Management Company

This function is needed for coordination with Budget.

b. Authorized User logs onto the System and selects the function.
c. System prompts for **Create**, **Modify** or **Archive Customer**.
d. User selects one of the following:
    1) **Create New Customer**
        a) System displays **New Customer** screen.
        b) User enters data.
        c) User indicates completion of data entry.
        d) System checks for duplicate entry and warns User when it is found.
        e) User reviews data.
        f) User can save entry or return to menu.
            e. The System assigns every Customer a unique Customer ID#. There may be need to coordinate this with NC accounting systems.
            f. If saved, new Customer immediately becomes available on relevant dropdown lists (e.g. new Maintenance Company appears on Maintenance Company dropdown lists).
    2) **Edit Customer**
        a) User searches for and selects Customer.
        b) System displays Customer data
        c) User modifies data
        d) User reviews data
        e) User can save entry or return to menu.
            g. If saved, revised customer data immediately become available to Users
            h. System saves history of old customer data
    3) **Archive Customer**
        a) This function exists to remove inactive Customers from dropdown lists but retain a record that they were once active.
        b) User selects the function.
        c) User searches for and selects Customer.
        d) User indicates that they are to be archived (i.e. no longer appear on related dropdown lists).
        e) System accepts the request.
        f) System enters the Customer in the archive list.
e. End of use case.

D. Budget Office

The System must:

- Help to maintain a clear segregation of responsibilities between Budget and the Back Office.
- Create a unique ID# for each invoice.
- Create a unique customer ID# that can be used by other state agencies (or use an ID# already created for that Customer).

1. Print invoices for Fees
    a. This use case is triggered when it is necessary to send invoices for Fees to Customers.
    b. Authorized person in Budget office chooses the function.
    c. System does a search for all records where an invoice must be issued (e.g. completed inspections; including inspections cancelled with less than 24 hours notice).
    d. System consolidates inspection fees for a single billing address to a single invoice:
        1) Individual inspections and related fees are detailed in the invoice.
    e. System makes the invoices available for inspection (soft copy).

f. System provides both mailing and email addresses, and defaults to sending a PDF copy of the invoice by email.
g. User inspects the invoices and can indicate those invoices that must be edited (in which case the System allows the User to edit the invoice).
h. User indicates completion of data entry.
i. System displays a summary of invoice data.
j. User reviews the data and has the option to:
    1) Edit the data.
    2) Submit the data.
    3) Cancel the request and return to menu.
k. System saves a submitted request.
    1) System prints the invoices that will be mailed to the applicant address (new inspections), maintenance address (alteration inspections) or billing address (all other inspections).
    2) System emails a PDF copy of the invoice to the applicant email address (new inspections), maintenance email address (alteration inspections) or billing email address (all other inspections).
    3) System notes in each record the date that the invoice has been sent.
l. User mails letters.
m. User can choose another function or exit the System.
n. End of use case.
o. Note: Applicant Company pays for the new device inspection; Maintenance Company pays for alteration inspections. Owner (at billing address) pays for all other inspections. System must be able to distinguish these different scenarios.
p. Note: System may have to interface with printer that folds invoices and stuffs envelopes.

2. Late Letters - Invoices
    a. This use case is triggered when one or more Customers have failed to pay their fee on time.
    b. Authorized person in Budget office chooses the **Late Payment** function.
    c. System displays a list of all pending letters sorted by number of days late.
    d. User reviews pending letters and indicates any that should be deferred or cancelled.
    e. For those invoices that are more than 45 days late, the User can have the System print a reminder letter along with a copy of the invoice with “Second Notice” added, and Budget Staff mails them. This letter is mailed to the billing address or the billing email address. System notes in each record that a reminder letter has been sent by entering the date sent. User can choose to send the letter by US Post or by email.
    f. For all invoices that are more than 60 days late, the User can have the System print a dunning letter along with a copy of the invoice with “Third Notice” added, and Budget Staff mails them. This letter can be sent by US Post or email. System notes in each record that a dunning letter has been sent by entering the date sent. It is acceptable to email the dunning letter.
    g. User indicates completion of data entry.
    h. System displays a summary of the data.
    i. User reviews the data and has the option to:
        1) Edit the data.
        2) Submit the data.
        3) Cancel the request and return to menu.
    j. System saves a submitted request.
    k. System prints or emails letters as directed.
    l. System records in each record the date that each letter is sent.
    m. The System automatically includes a facsimile of the authorized signature on the dunning letter.
    n. End of use case.

3. Refer late payments to NC Attorney General's office or collection agency
    a. This use case is used on a weekly basis.
    b. At least once each week, an authorized User in the Budget office runs a late payment function.
    c. For all invoices that are more than 120 days late:
        1) The System generates a report of all invoices that are over 120 days late for the first time.
        2) System compiles this information into a spreadsheet and makes it available for staff review.
        3) The User accepts the report or makes adjustments until it is acceptable.
        4) The User has the System send the spreadsheet to the NC Attorney General's Office (AG's Office) by email. The AG's Office sends a letter and that gives the late payer 30 days to pay.
        5) The System tracks the date of referral to the AG's Office.
    d. For all invoices where the Customer has not paid after being contacted by the AG's Office:
        1) The System generates a report of all invoices the Customer has not paid after being contacted by the AG's Office.
        2) System compiles this information into a spreadsheet and makes it available for Staff review.
        3) The User accepts the report or makes adjustments until it is acceptable.
        4) The User has the System send the spreadsheet to a collection agency by email.
        5) The System tracks the date of referral to the collection agency.
    e. End of use case.
4. Late Letters – Penalties
    a. This use case is used on a weekly basis.
    b. At least once each week, an authorized User in the Budget Office runs a late payment function.
    c. The System does the following:
        1) The System compiles a list of all Customers where it has been 30 days since the Penalty packet was sent AND a signed green card has been received AND the penalty has not been paid AND no informal conference has been planned.
            a) Budget User reviews list and makes adjustment as needed.
            b) Budget User has the System send a friendly reminder letter by US Post or email along with a copy of the original invoice that has been modified to include "Second Notice".
        2) The System compiles a list of all Customers where it has been 60 days since Penalty packet was sent AND a signed green card has been received AND the penalty has not been paid AND no informal conference has been planned.
            a) Budget User reviews list and makes adjustment as needed.
            b) Budget User has the System send a dunning letter along with copy of invoice by US Post or email along with a copy of the original invoice that has been modified to include "Third Notice".
        3) The System compiles a list of all Customers where it has been 90 days since Penalty packet was sent AND a signed green card has been received AND the penalty has not been paid AND no informal conference has been planned.
            a) Budget User reviews list and makes adjustment as needed.
            b) Budget User has the System print a judgment certificate, a letter that the Deputy Commissioner signs, and a letter that a Budget Official signs.
            c) Budget User sends the entire packet along with a copy of the citation to the Clerk of Court. Clerk of Court reviews, approves and returns the packet.
                i. System records date packet was sent to the Clerk of Court, and the date it is received back in the Budget Office.

d) When the packet comes back to Budget, the Budget Office User records the date it was received and has the System print a form letter to the Customer.
e) The entire packet and the form letter are all sent to the Customer via US Post. Customer is given 30 days to pay.
i. System records judgment date and date packet is sent to Customer.
f) If the Customer pays, Budget User records this in the System and has the System print a cancellation form and letter. These are sent to the Clerk of Court to cancel the judgment.
i. The Budget User has the System print a form letter to the Customer, and sends a copy of the cancellation documents along with the letter to the Customer.
ii. System records date of cancellation and date letter was sent.

4) The System compiles a list of all Customers where it has been 30 or more days after judgment was filed AND the Customer has not paid. The information is put into a spreadsheet and made available for Staff review.
a) The User accepts the report or makes adjustments until it is acceptable.
b) The User has the System send the spreadsheet to the NC Attorney General's Office by email. The AG's Office sends a letter and that gives the late payer 30 days to pay.
c) The System tracks the date of referral to the AG's Office.

5) The System compiles a list of all Customers where it has been 30 days since they were contacted by the AG's Office AND they have not paid.
a) System compiles this information into a spreadsheet and makes it available for Staff review.
b) The User accepts the report or makes adjustments until it is acceptable.
c) The User has the System send the spreadsheet to a collection agency by email.
d) The System tracks the date of referral to the collection agency.

d. End of use case.

5. Write off
a. This use case is triggered when Customer has not paid despite all actions taken.
b. Budget User runs the **Write Off** function. System displays a list of all Customers who have not paid as follows:
1) For fees and penalties without judgment:
a) If the account remains unpaid after three years, the account is past the statute of limitations and they are written off.
b) System records date of write-off.
2) For penalties with judgment:
a) If the account is five years past the judgment date, the account is written off. In this case, the physical file is discarded after 10 years.
c. User may scan all documents and links them to the record.
d. User sends hard copies of all documents for archive and records the archive information.
e. End of use case.

6. Process payment of invoices (Fees) - Checks
a. This use case is triggered when a Customer has paid by check.
b. Authorized person in Budget scans the check for deposit.
c. Scanner makes deposit and prints report of all checks deposited in that batch.
d. User delivers the report, checks and slips to the Budget Division Accounts Receivable Technician (AR Tech) to post to Elevator System. The AR Tech:
1) Enters information
2) Validates the information

3) Posts the checks
4) On posting, System generates 3 lists. User chooses how to sort each list.
    a) System prints one list to go to a second AR Tech for posting to NCAS, the central state accounting system.
    b) Second list printed to go into vault with checks. These lists are destroyed after 45 days.
    c) Third list is kept along with deposit report as backup. Kept for 3 years.

e. System notes any incorrect payments (e.g. duplicate payments, partial payments, over payments), generates a list (PDF file) and puts the list in the My Communications section of an AR Tech in Budget. The AR Tech resolves these discrepancies.
f. End of use case.

7. Process payment of invoices (Fees) – eChecks (pay with bank routing number and account number) and credit card payments
    a. This use case is triggered when a Customer has paid by eCheck or credit card.
    b. Authorized person in Budget runs the PayPoint system.
        1) When the payment is made from the Admin side, Budget User enters information into PayPoint. If approved, Budget User posts it into the Elevator System.
            a. Interface would be helpful here.
        2) When the payment is made by the Customer online, the System updates the Elevator System.
            a. This assumes that an interface is available.
    c. Daily, the AR Tech checks PayPoint reports to ensure that all payments actually went through. Payments that did not go through are posted manually to Elevator System
        1) AR Tech creates lists as described above.
    d. End of use case.
8. Process payment of invoices (Fees) – ACH
    a. This use case is triggered when AR Tech receives a list of ACH payments on paper.
    b. Authorized person in Budget posts the payments as described above.
        1) Enter
        2) Validate
        3) Post
        4) Create lists
    c. System notes any incorrect payments (e.g. duplicate payments, partial payments, overpayments), generates a list (PDF file) and puts the list in the My Communications section of AR Tech in Budget.
    d. AR Tech contacts the Customer to let them know about duplicate payment. Customer and Treasurer's Office take care of this.
    e. End of use case.
    f. Note the following:
        1) Some payments (by check, ACH, etc.) include payment for more than one agency, e.g. Boiler and Elevator (combos). These need to be sorted out.
        2) Budget needs to reconcile their Deposit Report with what goes into the Elevator System.
        3) Budget posts into NCAS for Elevator.
        4) Techs reconcile their postings once per week and monthly. They check their postings against NCAS.
9. Remove a payment – NSF Check
    a. This use case is triggered when a Customer's check is returned due to non-sufficient funds.
    b. AR Tech in Budget selects the function.
    c. User enters the invoice number.
    d. System removes the payment from the record.
    e. System notes the date of the returned check in the record.

f. User saves the record.
g. At end of day System compiles a report of all returned checks and puts it into the My Communications section of an AR Tech.
h. AR Tech calls the Customers with returned checks and requests payment.
i. User can elect to have the System print a form letter to the Customer regarding the returned check and resulting fee.
    1) AR Tech records the returned check fee in the System.
j. After 30 days, if the invoice is not paid, the System automatically determines how late the payment is and enters the correct status for that record. It now goes into the usual late payment cycle.
k. End of use case.

10. Process exceptions
    a. This use case is triggered when a Customer has made an incorrect payment (e.g. duplicate payment, partial payment) or when an invoice was sent to the wrong address.
    b. Wrong address: Invoice is returned to Budget. Budget logs this in the System. The issue is referred to the AR Tech to call the Customer to get the correct address. The AR Tech re-invoices with the correct address, via print or email.
    c. Duplicate payment: Deposited in bank but there is nothing to post to, so it goes into an unmatched account. AR Tech contacts the Customer to return payment. System records this.
    d. Partial payment: Budget tries to post the payment to the Elevator System, sees that there is a remaining balance. If the invoice is for one inspection, then the System posts the amount and provides the opportunity to print a remaining balance invoice. If there were multiple inspections, the System allows the AR Tech to apply payment to specific inspections until all of the payment is distributed, then a remaining balance invoice can be printed/emailed.
    e. End of use case.
11. Process Penalty payments – check
    a. This use case is triggered when a Customer pays a penalty by check.
    b. Works same as for Fees but applies to penalties only.
12. Process Penalty payments – eCheck
    a. This use case is triggered when a Customer pays a penalty by eCheck.
    b. Works same as for Fees but applies to penalties only.
13. Process Penalty payments – ACH
    a. This use case is triggered when a Customer pays a penalty by credit card.
    b. Works same as for Fees but applies to penalties only.
14. Process non-payment of Penalties
    a. This use case is triggered when a Customer fails to pay a penalty on time.
    b. Current process:
    c. Elevator sends a penalty notice out certified return receipt requested. If the Customer pays by check the payment goes to the AR Tech in the Accounts Receivable Group of the Budget and Management Division. The AR Tech handles all penalty payments; Elevator personnel are not allowed to process payments. Budget and Management does not have an accounting system to post the payment to; an Excel spreadsheet is used for this purpose. Once posted, the AR Tech sends a copy of the transmittal to the Back Office Staff in Elevator that the penalty has been paid. Note that there is no method to track the status of penalty payments in the current system. A second AR Tech codes the payment into the penalties budget code for Elevator in NCAS. Elevator Back Office Staff track these payments in a separate spreadsheet.
    d. At the end of month, the AR Tech reconciles to NCAS and makes certain everything matches, NCAS vs. Transmittal for Penalties. The AR Tech sends a Cost of Collections Report; the Department of Labor keeps a certain percentage of the penalties to pay for the

cost of collections. The rest of the money goes to the Office of State Budget and Management to be sent out to the counties.

e. Elevator sends a Penalty Packet (containing all paperwork sent to the Customer) to Budget when the packet is sent to the Customer the first time. The Customer has 30 days to respond. Customer must sign card and return it; Elevator sends the signed card to Budget so that Budget can continue the process. No collection takes place without a green card. The System informs the AR Tech when the invoice is paid. The System automatically starts the collection process if the invoice is not paid by the due date by creating a spreadsheet with relevant information and sending it to Budget. If the invoice is not paid, Elevator Staff can hand deliver an invoice if the Customer is not out of state; otherwise the penalty is not collectable because without the green card there is no evidence that the Customer received the notice. In this case the penalty has to be written off.
f. If there is a green card and the Customer has not paid,
    a. If it is past 30 days and payment is not received, a friendly reminder letter is sent
    b. If it is past 30 more days and payment is not received, a dunning letter is sent out.
    c. If it is past 30 more days and payment is not received, a judgment is filed against the Customer (a notice of final order with clerk of court with that county). Once filed, clerk of court mails the judgment back to Budget Office. A copy of the judgment and a letter is sent to the Customer. The Customer has 30 days to respond.
    d. If it is past 30 more days and payment is not received, the Attorney General's office sends out a letter giving 30 days for payment.
    e. If it is past 30 more days and payment is not received, the penalty is sent to a collection agency. Original invoice and reminder letter are automatically generated. For those penalties under $125.00 the System generates a spreadsheet with relevant information and sends it to a contact in the AG's office. If this fails, the System generates a spreadsheet with relevant information and sends it to a collection agency. Note: A penalty cannot be filed against a company address that is out of state, but it can be done by filing it against the in-state address where the work is done with that company's name.
g. End of use case.

15. Work with dropdown lists
    a. This use case is triggered when there is need to add or retire an item from a dropdown list. All dropdown lists in the System (except those maintained by Back Office) can be maintained through this function.
    b. Authorized User selects the function.
    c. User chooses a dropdown list.
    d. User chooses from **Add to List**, **Archive Item**, **Un-Archive Item**.
        a. **Add to List**: User enters the new item and selects **Save.**
        b. **Archive Item**: User chooses the item from the list and selects **Archive**. System marks this item with status **Archived**. Archived dropdown list items do not appear in any future use of the System (except this one) but are maintained in the System for prior records.
        c. **Un-Archive Item**: User chooses the item from the list and selects **Un-Archive**. System marks this item with status **Active**. Active dropdown list items appear in all future uses of the System.
    e. End of use case.
16. Create a new Budget User
    a. This use case is triggered when there is need to create a user ID and password for a new Budget employee.
    b. Only the AR Supervisor and IT are able to add Budget Users. Elevator Staff explicitly cannot add Budget Users.

E. Elevator Bureau Supervisors

1. Review Inspector work performance
    a. This use case is triggered whenever a Supervisor has need to review an Inspector's work performance.
    b. This use case might be satisfied by a series of predefined reports, rather than a specific system function. See list of suggested predefined reports with search criteria below.
        1) Performance reviews (number of new inspections, alterations etc over a defined period) by the day, week or month. Specify a range of dates. Have the ability to break down performance to specific items of interest.
        2) Analysis reports for route efficiency of Inspectors.
        3) Inspections overdue with breakdown by Inspector, region, type of equipment, etc.
        4) Have ability to look in real time at Inspectors work as the System is updated.
        5) Interim and year-end appraisal reports – System pre-fills an appraisal form with relevant information (e.g. time spent in various activities, production, performance log analysis).
    c. End of use case.
    d. Only the Bureau Chief and Assistant Bureau Chief should be able to see any of the Supervisor reports generated or Inspector performance-related info. No other Supervisors should be privy to this information without approval from that Supervisor or his superiors.
2. Supervisor gives permission to close down a device
    a. This use case is triggered when an Inspector has used the System to request permission to close down a device.
    b. NOTE: This is done verbally over the phone before the actual act of closing the unit (condemn or shutdown/ cert removal). Without connectivity statewide, a Supervisor cannot give real-time system permissions. Inspectors need the ability to do this. The report is submitted to the System, the report also goes automatically to the Supervisor for review just in case Inspector or Supervisor has no phone signal at the time of closing the unit and the Inspector forgets to call the Supervisor later in the day.
    c. Supervisor checks their My Communications section of the application.
    d. Supervisor selects and reviews the request.
    e. If the Supervisor agrees with the request they indicate this in the System.
        1) The System saves the decision in the record.
        2) The System puts the Supervisor's response as an alert in the My Communication section of the Inspector.
    f. End of use case.
    g. When this function is done by phone, this use case serves only to record the Supervisor's agreement to close down the device.
3. Assign one or more devices to a different Inspector
    a. This use case is triggered when it is necessary to assign a device to a specific Inspector, as when an Inspector becomes unavailable for inspections due to PTO. This use case can be also be used to optimize device allocation performed by the System. Transfer can be temporary until a specified date, or permanent. For the duration of the transfer, the System transfers all responsibility for the specified devices to the new Inspector.
    b. Authorized User (e.g. Supervisor, Bureau Chief) logs onto the System and selects the function.
    c. System displays a list of all Inspectors who fall under the person who logged in (e.g. Supervisor gets a list of only those Inspectors who report to them).
    d. User selects an Inspector.
    e. System prompts for entry of one or more **State ID#**.
    f. User enters one or more **State ID#s**.
    g. System displays current Inspector assigned to each device.

h. User indicates completion of data entry.
i. System displays a summary of the new assignment(s).
j. User reviews the changes and has the option to:
    1) Edit the request.
    2) Submit the request.
    3) Cancel the request and return to menu.
k. System saves the submitted request:
    1) Devices are assigned to the new Inspector.
    2) The same devices are removed from the original Inspector.
    3) If a device that falls in Supervisor A's region is assigned to an Inspector of Supervisor B e.g. by the Bureau Chief, Supervisor B is given the rights to work with the Inspector on that device.
l. System places an alert in the My Communications section of the affected Inspectors listing the change in assignment.
m. Once the User submits the request, they can choose another function or exit the System.
n. End of use case.

4. Supervisor defines an inspector territory (i.e. assign a set of devices to each Inspector).
    a. This use case is triggered when it is necessary to assign devices to an Inspector, as when a new Inspector is hired, an Inspector moves their home location or when there is need to rebalance the device load among Inspectors.
        1) Note: current territories are based on county boundaries. The following ignores those boundaries and attempts to provide each Inspector with a set of devices appropriate to their location and the density of devices in their area, i.e. Inspectors in rural areas who have more travel should be assigned fewer devices than those in an urban setting.
        2) Note: this function must consider both elevator and amusement devices.
    b. Authorized User logs onto the System and selects the function.
    c. System presents a list of all Inspectors.
    d. User selects Inspectors who will be affected by the change, or selects **All**
    e. User indicates completion of data entry.
    f. The System uses the current distribution of devices, takes note of the home location of each Inspector, and uses other parameters (to be defined) to reassign devices in an equitable manner (method to be defined).
    g. System displays a summary of the changes in the form of a map with:
        1) Office location of each Inspector
        2) Boundary of their new territory
        3) Number of elevator devices assigned to each Inspector
        4) Number of amusement devices in permanent facilities assigned to each Inspector
        5) Projected number of transient amusement devices assigned to each Inspector
    h. User reviews the changes and has the option to:
        1) Edit the request.
        2) Submit the request.
        3) Cancel the request and return to menu.
    i. System saves a submitted request.
    j. Once the User submits the request, they can choose another function or exit the System.
    k. End of use case.
    l. If a Customer has not yet contacted the original Inspector for a first inspection, the System sends the Customer an email with contact information for the new Inspector.

F. Elevator Bureau Management

Note: The Assistant Bureau Chief has access to all Bureau Chief functions.

1. Bureau Chief reviews variance request
    a. This use case is triggered when a Customer requests a variance from code. There are four participants in this use case: Bureau Chief, Inspector, Customer and System.
    b. When a User completes a variance request, the System generates a report and leaves it in the My Communications section of the Bureau Chief.
        1) Report includes information from the Customer, State ID #, and name of Inspector.
    c. If Bureau Chief agrees to consider the request, he/she uses a system function to forward the request to the Inspector's My Communications section.
    d. If Bureau Chief does not approve the request, he/she indicates this in the System and the System sends notice (by email if available, otherwise by printed letter) of this to the Customer.
    e. The Inspector does a site visit, enters information related to the inspection in the System and saves the data.
        1) The System has a special screen for entry of **Variance Request Site Visit** data.
        2) There is no fee for this visit.
    f. The System forwards a report of the site visit to the My Communications section of the Bureau Chief.
    g. The Bureau Chief reviews the report. If the Bureau Chief decides to approve the request, he/she indicates this in the System. He/she may also include information about specific work the Customer must do.
        1) The System records the then-current version of the code to which the variance(s) pertain.
    h. The System forwards notice of the approval to the My Communications section of the Inspector. The Inspector then tells the Customer the terms of the approval (e.g. specific work to be done).
    i. The Inspector checks the work required by the approval during the new device inspection.
    j. End of use case.
    k. Note: The System must display variance data as a standard part of information about any device so that Inspectors are aware of variances before inspections are done. The specific code version is displayed along with each variance.
2. Bureau Chief reviews Supervisor performance
    a. This use case is triggered when management wants to review the performance of one or more Supervisors.
    b. It should be possible to satisfy this function through use of reports.
    c. End of use case.
3. Bureau Chief reviews a proposed penalty
    a. This use case is triggered when an Inspector has proposed that a penalty be levied against an Owner or Elevator Company.
    b. The Bureau Chief opens the document in his/her My Communications section and reviews the report.
    c. The Bureau Chief asks Inspector about the level of cooperation of the Owner or Elevator Company, details of the incident, months without violations, number of people in company, etc.
    d. The Bureau Chief calculates a deduction from the proposed penalty calculation and enters a final penalty calculation (version 1) in the System.
    e. The Back Office prints proposed final penalty calculation (version 1) and sends to Owner or Elevator Company.
    f. Owner or Elevator Company has 15 days to review and request a negotiation or make payment. If they make payment at this point, this use case ends.

   g. If negotiation is requested, the Bureau Chief or Assistant Bureau Chief meets with Owner or Elevator Company and may a) develop a plan for correction of practice; b) further reduce the final penalty calculation version 1 to create version 2, or waive it altogether pending completion of correction plan.
   h. The Back Office enters correction plan into the System.
   i. When the Bureau Chief or Assistant Bureau Chief receives confirmation that the correction plan is completed, they enter final penalty version 2 into the System.
   j. System posts a copy of plan and final penalty in Budget My Communications section.
   k. End of use case.
4. Authorized User manages Back Office Staff user ID and password
   a. This use case is triggered when there is need to create a user ID and password for a new Back Office employee.
   b. This function can be performed by Back Office Supervisor, Bureau Chief or Assistant Bureau Chief.
   c. This function must be designed to be in compliance with standard IT requirements.
   d. Details to be determined during the business process reengineering.
   e. End of use case.
5. Create a new System Administrator
   a. This use case is triggered when there is need to create a user ID and password for a new System Administrator (“SysAdmin”).
   b. This function can be performed by Bureau Chief or Assistant Bureau Chief.
   c. This function must be designed to be in compliance with standard IT requirements.
   d. Details to be determined during the business process reengineering.
   e. End of use case.
6. Bureau Chief reviews request to keep certificate of operation away from device
   a. This use case is triggered when the System places an alert in the My Communications section of the Bureau Chief indicating that an Owner or Owner Representative has requested to keep one or more device certificates away from the device, e.g. in a central office. This may be done when there is concern about theft, vandalism, etc.
   b. Bureau Chief opens and reviews the alert.
   c. If the Bureau Chief agrees with the request, Bureau Chief contacts Owner and tells the Owner what is required.
   d. If the Bureau Chief objects to the request, Bureau Chief contacts Owner and tells the Owner that the request is denied.
   e. Bureau Chief notes the decision in the System.
   f. Note: Bureau Chief can delegate this work to Assistant Bureau Chief or Supervisor by forwarding the request in the System to their respective My Communications section.
   g. End of use case.

G. Shared Functions

The following use cases may be used by more than one role. Specific authorities to perform specific functions are yet to be defined.

1. Run ad hoc reports
   a. This use case is triggered when authorized Staff chooses to perform an ad hoc report. Who is authorized to run which report will be detailed later in a CRUD analysis.
   b. The System displays a report-builder screen.
   c. The User defines the report.
   d. The User enters search parameters and runs the report.
   e. The System displays the results.

f. The User has the options to:
    1) Print report data to printer.
    2) Save report data to file (e.g. Excel or PDF).
    3) Name, describe and save the ad hoc report to be used again later as a predefined report.
    4) Define another ad hoc report.
    5) Exit the function.
g. End of use case.
h. Note: the ad hoc report System must allow search on all data in the System, including archived data.

2. Run predefined reports
    a. This use case is triggered when authorized Staff chooses to perform a predefined report. Who is authorized to run which report will be detailed later in a CRUD analysis.
    b. The System displays a list of available predefined reports.
    c. The User enters search parameters and runs the report.
    d. The System displays the results.
    e. The User has the options to:
        1) Print report data to printer.
        2) Save report data to file (e.g. Excel or PDF).
        3) Run another predefined report.
        4) Exit the function.
    f. End of use case.
3. Run canned reports
    a. This use case is triggered when authorized Staff chooses to perform a canned report. Who is authorized to run which report will be detailed later in a CRUD analysis.
    b. The System displays a list of available canned reports.
    c. The User chooses and runs the report.
    d. The System displays the results.
    e. The User has the options to:
        1) Print report data to printer.
        2) Save report data to file (e.g. Excel or PDF).
        3) Run another canned report.
        4) Exit the function.
    f. End of use case.
4. Zip code lookup
    a. This use case is triggered when a User needs the zip code for an address.
    b. Optional: could be link to third party application.

H. Public Functions

The following use cases may be used by the general public.

1. Citizen enters a Freedom of Information Act (FOIA) Request
    a. This use case is triggered when someone in the general public wants information about elevators, inspections, companies owning or operating elevators, etc. that might be stored in the System.
    b. User navigates to the public interface and selects the **Information Request** function.
    c. System displays a **Freedom of Information Request** form.
    d. User fills in the form.
    e. When the User has entered all required data, User may:
        1) Review and edit the information.
        2) Submit the information. When the information is submitted:

a. The System puts a message in the My Communications section of the Back Office Staff informing them of a FOIA request.
b. The User may print the submitted information and/or save it to file on their local computer (e.g. as PDF).

3) Cancel the request and return to the menu.

a) End of use case.

IV. Reports

The following indicates the range and types of reports that will be required. The lists are not intended to be all inclusive.

A. Ad hoc reporting

1. The System must provide a means for authorized system Users to query the database in an ad hoc manner. This includes the following:
    a. System presents a list of data elements which can be used as search criteria. User indicates which are to be used in the search (e.g. date range) and enters the search criteria data (e.g. two dates).
    b. System presents a list of data elements which can be included in the report. User indicates which are to be used.
    c. User specifies which report elements the System should use for sorting, with up to three levels of sorting available.
    d. Specify for each sorting element the direction of sort, e.g. lowest to highest; most recent to oldest.
2. System must display report results on the computer screen and allow the User to review the data.
3. User must have the options of printing the report, saving the report to PDF or Excel, or exiting the report.
4. Users must be able to name, describe and save ad hoc reports for later use. These saved reports should be added to a list of saved ad hoc reports.
5. It must be possible to search and report on any data element in the database.
6. Examples of ad hoc reports:
    a. Report on what people are requesting that the Back Office Staff look up, e.g. how many requests have we received involving valves?
    b. How many cases of late fee payment did we have in Region 3 in the first quarter?

B. Pre-defined reports with search criteria

1. Predefined reports must be available in a list, and an authorized User must be able to select and run a report. These reports can operate as follows:
    a. The User selects the report.
    b. The User inputs a value or a range of values for specified data elements that the System uses as search criteria.
    c. The System performs the search.
    d. The System uses found data to populate a predefined report.
2. System must display report results on the computer screen and allow the User to review the data.
3. User must have the options of printing the report, saving the report to PDF or Excel, or exiting the report.

The following are examples of the kinds of reports that must be delivered with the System.

1. List of inspections due:
    i. Authorized User searches for inspections due in any or all of the following categories.
        1) New inspections
        2) Routine inspections
        3) Alteration inspections
        4) Compliance inspections
    j. User can choose to specify a range of dates.
    k. User can specify other data such as Inspector, device Owner, Local Contact, etc.
    l. The System finds and displays the appropriate device records, sorting by inspection type and date with the most overdue first.
    m. User can save this report in PDF, print the results, rerun the report or exit the function.
2. Information on recalls of one or more devices.
3. Inspection report – a one-page report that an Inspector leaves with a Customer after completing an inspection.
4. Inspection data – data about the inspections completed by one or more Inspectors.
5. Device history – summary of any or all of the following for a device: permits, inspections, fees (and related actions) and penalties (and related actions) within a date range.
6. Violations report – a report that lists all violations in the chosen region or by Inspector, by date range, by violation type, etc.
7. Performance metrics on an inspection – Supervisor can obtain information on how an Inspector is doing through a report on metrics, e.g. hours spent on inspections, travel, conference, etc.; number of inspections done in a day / week; percent of devices in rollover status or in given time ranges of days overdue; status of paperwork.
8. Time metrics for an Inspector – Supervisor can obtain specific time data for one or more Inspectors, specifically work time, PTO, comp time earned / used, etc. Supervisor can save reports specific to each Inspector with selection criteria specific to each.
9. Overdue Penalties list – Authorized User can obtain a list of all overdue penalties sorted by amount overdue (e.g. 30, 60 and 90 days) with details about the Customers involved and actions already taken.
10. Track returned check fees – A list of returned checks and fees collected or in collection within a time period, with data on device Owners, etc.
11. Rollovers per region - Authorized User can obtain a list of all rollovers in a region, sorted by Inspector and amount overdue.
12. Check billing history - Details to be determined during the business process reengineering.
13. Monthly report - Details to be determined during the business process reengineering.
14. Quarterly report - Details to be determined during the business process reengineering.
15. Yearly report - Details to be determined during the business process reengineering.
16. Track fee payments, e.g. list of fee payments coming due, due now, overdue, etc.
17. Track fine payments, e.g. list of fine payments coming due, due now, overdue, etc.
18. Accident report –provides all relevant information about any recorded accident. Enter the State ID# and a list of accidents is displayed. Choose one or more accidents and full reports are displayed with option to print, email, etc. Data include all text, pictures, scanned documents, etc.
19. Accident tracking – report that provides a list of all accidents that fall within the specified selection criteria, e.g. date range, Inspector, Owner, physical address, etc.. User can drill to detail from list.
20. Returned check report – list of all Customers with a returned check that still have not paid
21. Late payment report – list of all Customers who have not paid sorted by how late they are, e.g. more than 45 days, more than 60 days, etc.
22. List of all recalls associated with a manufacturer model / release.

23. Track variances report – Could be used to analyze which devices have the largest and smallest number of variances. Search criteria could be Inspector, region, device type, date range, manufacturer, etc.
24. Track penalties report – Used to get a list of one or more devices with unpaid penalties. Search by location, date range, Inspector, etc. Report shows history of the penalty fee, e.g. letters sent, actions taken, current status.

In addition to the above, Supervisors need reports that can answer the following questions:

a. Has the Inspector filled out reports properly?
b. What did the Inspector do that day or week?
c. Is he keeping up his database?
d. How is he charging his time?
e. Is time coded properly? Elevator and amusement travel and field; are they coded properly? Current input is susceptible to putting data in wrong place.
f. Are they efficient in their daily travels? Good use of time?
g. Are expenses reasonable? Is number of miles reasonable given work done?

C. Canned reports

Canned reports are reports that are run without the need to specify search parameters. Examples include:

1. Permit – a one-page document that allows the construction company to complete work on a device. For new devices the form may include a facsimile of an ink “Approved” stamp. The System creates this as a PDF file and emails it to the applicant, who prints the file and posts it at the job site. Office Staff must be able to run this same operation as a report.
2. Approved application – when the Engineer approves of a new permit, the System creates a PDF file of a completed application and emails it to the applicant. Office Staff must be able to run this same operation as a report.
3. Inspection report – a one-page report that an Inspector leaves with a Customer after completing an inspection.

D. Automatic reports and other actions

Automatic reports and actions are triggered by elapsed time or some other event and automatically run by the System. Report output is placed in the My Communications section of the application. Examples include:

1. Daily Inspector performance report – includes a list of all inspections done by that Inspector on that day (e.g. date, Inspector name, 8 elevators done, State ID # and location of each, etc). Sent to the Inspector’s Supervisor.
    - Note: In current System this is generated by the Inspector laptop and used by Back Office Staff to ensure that nothing was missed, e.g. if report says 8 inspections were done are they actually in the System.
2. Automatic notification that permit is about to expire. Sent xx days before a permit will expire and informing the Customer on how to get an extension if one is needed.
3. Daily Total Fees Assessed by Inspectors is an automatic daily report that is sent to the Authorized User in Budget. They find it in their My Communications section of the application.
4. Weekly Total Fees Assessed by Inspectors is an automatic weekly report that is sent to the Authorized User in Budget. They find it in their My Communications section of the application.
5. Automated list of elevators with five-year inspection due.

E. Graphs and Charts

The System shall provide basic capability to display data as graphs and charts, e.g. histograms, pie charts, scatter diagrams, bar charts.

V. Transition Requirements

Transition requirements are those requirements that are relevant only at the time of system delivery, i.e. at the time that ownership of the System is transferred from the project team to the Customer. The following transition requirements have been identified; others may be discovered during detailed requirements analysis.

1. Import at least 10 years of data.
2. Some current data are not stored in the legacy System, e.g. accident data before 2006. These are primarily stored in spreadsheets.
3. Old variances are not recorded in the legacy System. They do not have to be put into the new System – too much data entry. Variances will be tracked from now forward.
4. Data in the legacy System will require cleansing before transfer to the new database
5. There are numerous duplicate addresses in the System. These need to be cleansed as part of data migration.

VI. System / Process issues

The following are areas of complexity that must be resolved or defined in the new System.

C1. Current process: laptops and printers are a weak point. Heat kills the equipment. Some Inspectors do not bring the laptop to the elevator, have to go back and forth to print, may have parked blocks away from the inspection site. Printers break.

C2. Current System: only Inspectors are allowed to update addresses except for billing which must be done by Budget. It is true that Inspectors may be the ones to find out about an address change (Owner and Local Contact change a lot) and it is convenient for them to update the address when there is only one change. But sometimes there is a need to update over 100 addresses due to the change in Owner. Responsibility for address changes needs to be resolved.

C3. There have been cases when apparently good addresses were rejected by the post office. New System should have some sort of formatting check on addresses.

C4. There was a request for a handheld device that includes a bar code reader. Put a bar code on the certificate, scan the bar code and that identifies the device, brings up the record. Input data on the handheld device and it prints a receipt that does the job of the current inspection report. This could all be done on the premises, saving trips back to the car for printing.

C5. Current System: any Inspector can pull up records of any other Inspector. The System should restrict access so each Inspector can only see their own data. A Supervisor can allow one Inspector to see another Inspector's devices when they are not available to do the work.

C6. Ensure that the process described in the Use Case Scenarios above fully supports **13 NCAC 15 .0104 NOTIFICATION OF DECISION BY OWNER OR OPERATOR** (a). of the Elevator Safety Act.

C7. The wording on the printed certificate changes depending on the circumstance. See **13 NCAC 15 .0202 EXISTING INSTALLATIONS OF ELEVATORS, ESCALATORS, DUMBWAITERS AND MOVING WALKS, ALTERATIONS, REPAIRS AND EXCEPTIONS.**

C8. **13 NCAC 15 .0303 CONSTRUCTION PERMITS** requires that the permit application be in triplicate and that all plans be in duplicate. This may not apply any more. This issue must be resolved during the business process reengineering.

VII. Interfaces

The following is a list of interfaces that may be relevant to the new System.

I1. An interface to the Filenet system (or the equivalent if Filenet is replaced) is required. This system holds engineering drawings, photos related to accidents and other materials.

I2. An interface to the ACH system used in Budget is needed. Currently, after Budget pulls down the ACH data, a deposit report is posted manually in the Elevator System. This is done daily.

I3. An interface to PayPoint may be needed for management of payments by eCheck.

I4. If a new accounts receivable system is implemented, an interface will be needed.

I5. An interface with the collection agency is needed. They prefer a spreadsheet.

I6. An interface with the AG's Office is needed. The AG's Office WANTS a spreadsheet until a different system is adopted. The proposed interface is unknown at this time; will likely be XML.

I7. There is a request for an interface to the State Motor Fleet; however, the State Motor Fleet has not developed an electronic interface at this time. This request is on hold until such time.

I8. The public interface needs definition. There are complexities in the relationships among parties (Owners, Local Contacts, repair people) and how the system will track who can affect which devices, what happens when Owners or Local Contacts change, etc. Details need to be determined during business process reengineering.

I9. There may be need for an interface with a state-wide accounting system through which all agencies share unique ID# for each Customer.

VIII. Data Requirements

Data requirements include the characteristics of specific data elements of the database. The following data have known special requirements. It is expected that other data with special requirements will be discovered or defined during detailed requirements analysis.

Z1. Equipment Type – This is specified in the permit request. There are 11 equipment types in the legacy System, and each type has been assigned a number as follows:

1 – Special equipment

2 – Belt lifts

3 – Dumb waiter

4 – Escalator

5 – Freight equipment

6 – Passenger equipment

7 – Handicap lifts

8 – Moving walks

9 – Orchestra lifts

10 – TV towers (under moratorium – stopped inspecting because of hazards)

11 – Temporary hoist (for outside construction)

The new System must include all of the above. In addition, the new System must allow editing of existing equipment types and creation of new equipment types. It must be possible to remove an Equipment Type from the drop list but retain existing information related to that equipment type.

Z2. A uniform State ID numbering system is required. Every piece of equipment must have a unique State ID#.

Z3. Every device has an operation type. There are several operation types defined in the legacy System (e.g. hydraulic type elevator; friction type elevator). The new System must include all existing operation types. In addition, the new System must allow editing of existing operation types and creation of new operation types. It must be possible to remove an operation type from the drop list but retain existing information related to that operation type.

Z4. Every device must have a link to engineering drawings. These drawings are currently kept in the Filenet system.

Z5. Variance from code is a new data element tied to a device record and associated with permit request for alteration. Variance is tied to the version of the code in effect at the time they pass inspection. Variances last forever and must be visible for the Inspector to see when they are preparing for an

inspection. System is to record that a specific request has a variance associated with it along with details on the variance and actions taken on it.

Z6. Local contact is a new data element. This is the person that the Inspector has identified as easiest to contact. Includes name, phone, email, etc. There can be more than one local contact for a device.

Z7. Every device has a text name as well as a unique State ID#. This makes it easier for Owners to know, for example, which elevator is which.

Z8. Data in the legacy System are not normalized; the data structure will have to be redesigned.

Z9. State ID#s in the legacy System involved use of four different numbering schemes. These must be rationalized into a single numbering scheme in the new System. Numbering schemes in the legacy System are as follows:

a. Standard devices use a 5 digit number
b. Handicap lifts have the prefix H and their numbers start with 2000
c. Temporary lifts have the prefix A and their numbers start with 500
d. Elevators that were discovered to be non-registered have the prefix N + the county code 1 to 100 plus a unique number. There are about 1000 of these.

Z10. There are four different address types in the legacy System: Applicant, Owner, Occupant and Billing. The storage of these addresses is based on an idiosyncratic numbering scheme that will have to be replaced.

Z11. Inspectors are currently required to code every inspection by inspection type. But some of the inspection types in the current System sound more like device status (see device statuses in the Change in State section below). This needs to be redefined. Current inspection types include:

1 – New, 2 – routine, 3 – compliance, 4 – modification but covers alterations and repair, 5 – not inspected; 6 – properly landed, as when it is put out of service; 7 – condemned, not in use and not safe to use but want to keep it live; 8 – removed from service, used when Owner has been evasive or Inspector can't get in building and DOL takes the device out of service with a sticker; 9 - destroyed

Z12. Certificate statuses listed below under Changes in State are not consistent with current usage. This discrepancy requires resolution.

IX. Technical Requirements

Technical requirements are those requirements that pertain to the conditions under which the new System will operate, and to certain technical characteristics of the new System. The following technical requirements have been identified; others may be discovered during detailed requirements analysis.

TR1. Manage authorized Users of the new Elevator System via integration with Microsoft Active Directory.

TR2. Inspectors must have access to System data related to their inspections at all times. Full-time access to the main System via wireless broadband to/from the Inspector's laptop in the field is not currently viable, given the lack of acceptable signal strength from current providers. Elevator Inspectors cover every county in the state; uninterrupted wireless access cannot be assumed in many areas. Proposed Systems must take this constraint into account.

TR3. It is not mandatory for the System to allow access in real time to data that is updated in real time. It is sufficient to query local data (e.g., on the Inspector's laptop) that is updated daily.

TR4. Direct entry of inspection results into the mobile device by the elevator Inspector. Double data entry should not be required (e.g., from paper to computer, or rekeying from one application to another). Caching inspection results on the mobile input device for daily uploads is acceptable.

TR5. The System must support field printing of inspection reports and certificates of operation.

TR6. The System must support the ability to integrate geographic information system (GIS) and global positioning system (GPS) capabilities. GPS will be used by Inspectors to determine optimum routes and minimize travel time. The optimal system will be able to integrate with locally-installed GPS software to allow for real-time navigation and scheduling decisions by the Inspector on the road.

X. Changes in State

There are several aspects of this System that change state depending on actions or lack of action by various actors. The following are proposed for the new System:

Record Status

1. A device can have the following statuses:
    - **Standard Certificate Application** Customer has requested an inspection for a standard certificate.
    - **90 Day Certificate Application** Customer has requested an inspection for a 90-day certificate.
    - **New Permit Approved** when the permit application is first approved.
    - **Pending First Inspection** after the Installer contacts the Inspector and has made arrangements for an inspection.
    - **Active** after the first inspection (Note: this status is **Closed** in the legacy System, probably referring to the permit application).
    - **Shutdown** for significant violation; certificate is removed.
    - **Locked down** device is physically locked down due to an imminent threat to public safety.
    - **Properly Landed** when it is permanently Out Of Service per NCAC.
    - **Condemned** when it is not in use or not safe to use but want to keep it live. (This can happen when the device is unsafe and the certificate has been removed for a year, OR no power for a year. NCAC requires Proper Landing. Inspector can go back annually and charge inspection fee till Properly Landed).
    - **Removed from Service** when the Owner has been evasive or Inspector can't get in the building or a fee is more than 90 days overdue and DOL takes the device out of service with a sticker.
    - **Destroyed** when the device has been demolished and no longer exists.

    Note: the only device statuses used in the legacy System are **Open** and **Closed**.
2. A Certificate can have the following statuses:
    - **Not Issued** before the first inspection of a new device.
    - **Issued** after the first inspection and the certificate has been placed in the device.
    - **Re-issued** after a routine inspection and the certificate is still active.
    - **Compliance** when an infraction was found and the Owner is given a limited amount of time to do a repair. Once the repair is completed the status changes to **Re-Issued.**
    - **Limited** when a 90-day certificate has been provided so that the device (elevator) can be used for construction. When the time is up the status goes back to **Not Issued** if an inspection has not been done.

- **Decertified** when a renewed 90-day certificate runs out, if the elevator is not completed then the Inspector removes the certificate.
- **Removed** when the Inspector removes a certificate from the device due to a serious violation.
- Note: these statuses should be reviewed for possible change.

3. A Permit can have the following statuses:
   - **Active** from the time it is issued and lasting two years.
   - **Extended** from the time it is re-issued and lasting 2 years.
   - **Expired** once it has expired.
4. A Fee in a record can have the following statuses:
   - **SendInvoice** if the fee is due but no invoice has been sent.
   - **InvoiceSent** after an invoice has been sent.
   - **FeeLate1** when an invoice has not been paid after 45 days. This triggers a reminder letter (Budget).
   - **FeeLate2** when an invoice has not been paid after 60 days. This triggers a dunning warning letter. (Budget).
   - **FeeLate3** when an invoice has not been paid after 90 days. This triggers a dunning letter (Back Office).
   - **Revoked** when an invoice has not been paid after 120 days and an Inspector has removed the certificate from the elevator.
   - **Paid** when the Fee has been paid.
5. A Penalty in a record can have the following statuses:
   - **SendInvoice** if the Penalty is due but no invoice has been sent.
   - **InvoiceSent** after an invoice has been sent.
   - **PenaltyLate1** when an invoice has not been paid after 30 days. This triggers a reminder letter (Budget).
   - **PenaltyLate2** when an invoice has not been paid after 60 days. This triggers a dunning letter (Budget).
   - **PenaltyLate3** when an invoice has not been paid after 90 days. This triggers a judgment against the Customer (notice of final order with clerk of court with that county).
   - **PenaltyLate4** when an invoice has not been paid after the judgment. This triggers a second dunning letter (Budget).
   - **PenaltyLate5** when an invoice has not been paid after the second dunning letter. This triggers referral of the matter to a collection agency.
   - **Paid** when the Penalty has been paid.

XI. Business Rules

Business rules are statements of policy that must be enforced by the System. They may also be guides on how to determine whether a value is true or false.

The following are known business rules that will impact the design and operation of the new System. It is expected that additional business rules will be discovered or defined during a detailed requirements analysis.

B1. A permit for installation of a new device is good for 2 years. This is included on the permit that is printed and posted on the job site.

B2. A certificate of operation is valid until the next inspection (i.e. there is no expiration date). Annual inspection is required by statute.

B3. A record must be kept of the Inspector who does each inspection.

B4. Device Company pays for the new device and alteration inspections. Owner pays for all routine inspections. Owner is responsible for payment no matter who the Owner delegates for this action such as a management company.

B5. There is never a fee for a routine compliance inspection.

B6. Every new or alteration inspection costs $200.

B7. Regular device inspections cannot be done more often than every 6 months (per the Elevator Safety Act).

B8. Every device must have a certificate of operation.

B9. The System must store whatever plans and diagrams that are deemed necessary to support a permit request.

B10. Condemned or landed units that have been out of service and not continuously maintained for more than one year, then it must pass inspection before a new certificate is provided.

B11. Whenever action is taken under section 95-110.6.of the Elevator Safety Act, the affected party shall be given notice of the availability of an administrative hearing and of judicial review.

B12. Penalties of varying amounts can be levied for the following:

a. Operation without a valid certificate or operation not in accordance with Article or rules and regulations.
b. Operation after refusal to issue a certificate or revocation of a certificate.
c. Failure to report death, injury or device damage within 24 hours.
d. Owner cannot be notified of a penalty by email. Notice must be via US Post (see Article for details).

B13. A penalty cannot be levied on a company that is out of state.

B14. Existing devices must be maintained under the standards in effect at the time of their installation.

B15. An Inspector cannot do a current routine inspection if last year's invoice has not been paid.

B16. Any of the following roles can request Modifications of devices:

a. Owner
b. Maintenance Company
c. Property Management Company

B17. The System assigns every device a unique State ID# .

Note the following:

a. Existing devices already have a legacy State ID#.
b. Legacy State ID#s are alphanumeric.
c. The numeric portion of legacy State ID#s is not unique.
d. The alpha portion of legacy State ID#s is used to denote special equipment.

B18. A 90-day certificate of operation can only be assigned to one class of device: elevators.

B19. Engineer must record the date that an alteration permit is approved. That is what determines the code violation document that is in effect for the subsequent inspection.

B20. A Compliance inspection is required whenever there are one or more significant violations in a routine inspection.

B21. The System must inform the relevant Supervisor of all instances of certificate removal, shutdown or condemnation.

XII. Roles

The following are known roles that are needed in the new System. It is possible that additional roles will be discovered or defined during a detailed requirements analysis.

1. Inspector
2. Supervisor
3. Manager (Bureau Chief and Assistant Bureau Chief)
4. Back Office Staff – Office Manager
5. Back Office Staff – Office Assistants
6. Back Office Staff – Engineer
7. Back Office Staff – Application Administrator
8. System Administrator
9. Budget – Collections Officer
10. Budget – Accounts Receivable Technician (“AR Tech”)
11. Customer – Owner
12. Customer – Property Management Company
13. Customer – Local Contact
14. Customer – Device Company
15. Customer – Device Maintenance Company

XIII. Existing Database Schema

This section describes the most important tables in the existing elevator inspection-processing system for the NCDOL Elevator and Amusement Device Bureau. The intent of this section is to assist Vendors in estimating the level of effort required to migrate existing inspection data to any new system proposed.
Note:

- This schema only shows tables related to elevator inspections; amusement device tables are not included.
- Total size of this database is < 500MB.
- Number of records indicated for each table may vary from the current state of the database.
- Additional tables related to elevator inspections exist in this schema beyond the ones shown in this documentation. The other tables are either lookup tables, sparsely populated or obsolete, and are omitted for the sake of clarity.

- The existing tables are not fully normalized. Migration estimates must take this fact into account, and must include additional time for sufficient analysis to map existing data to a properly normalized state in any new system.
- Notation conventions for each table are as follows:
  - The table name is listed first in capital, bold letters: **ELEV_ELEVATOR**
  - Column names follow, enclosed in parentheses.
  - Primary keys, where known, are underlined: STATE_ID
  - Foreign keys, where known, are marked with an asterisk: COUNTY_CODE*

ELEV_COMPANY_ADDRESSES (NAME_CODE, NAME, ADDRESS1, ADDRESS2, CITY, STATE, ZIP_CODE, TITLE, F_NM, L_NM, NAME2, EMAIL, PHONE, FAX) ***Number of Records = 80,771***

ELEV_COUNTY (COUNTY_CODE, COUNTY_NAME) ***Number of Records = 100***

ELEV_COUNTY_INSPECTOR (COUNTY_CODE, COUNTY_AREA, INSPECTOR_CODE*) ***Number of Records = 116***

ELEV_DAILYDETAIL (INSPECTOR_CODE, INSPECTION_DATE, PERIODIC_ELEVATORS, PERIODIC_DUMBWAITER, PERIODIC_ESCALATOR, PERIODIC_HC_LIFTS, PERIODIC_BELT_LIFTS, PERIODIC_COMPLIANCE, PERIODIC_WITNESS_TEST, PERIODIC_REMOVED_FROM_SERVICE, PERIODIC_CERT_ISSUED, NEW_ELEVATOR, NEW_DUMBWAITER, NEW_ESCALATOR, NEW_NC_LIFTS, NEW_BELT_LIFTS, NEW_HOIST, NEW_ALTERATION, NEW_COMPLIANCE, NEW_CERT_ISSUED, ELEVATOR_CONDEMNED, ELEVATOR_LANDED, ELEVATOR_DESTROYED, ACCIDENT_INVEST, AMUSEMENT_DEVICE_INSPECTION, TRAMWAYS_ROPE, TRAMWAYS_CHAIR, TRAMWAYS_J-BAR, TRAMWAYS_T_BAR, TRAMWAYS_INCLINE, TRAMWAYS_OTHERS, TRAMWAYS_COMPLIANCE, TRAMWAYS_CERT_ISSUED, FEES_COLLECTED, TRAVEL, FIELD, OFFICE, ANNUAL, SICK, COMP, HOLIDAY, SUPERVISORY, CONFERENCE_HOURS, TOTAL_MEALS_LODGING_OTHER, ODOMETER_NET, MILEAGE_RATE, CONFERENCE_EXPLANATION, FIELD_AMUSE, I_COMMENTS, INFLATABLE_INSPECTION) ***Number of Records = 38,949***

ELEV_ELEVATOR (STATE_ID, COUNTY_CODE*, COUNTY_AREA, ELEVATOR_TYPE, OPERATION_TYPE, CAPACITY, INSTALLED_DATE, COMPLIED_DATE, CERTIFICATE_STATUS, UI, STATE_OWN, OWNER_CODE*, OCCUPANT_CODE*, EQUIPMENT_TYPE, DRIVE_MACHINE, VOLTS, SPEED, FLOOR_FROM, FLOOR_TO, LANDINGS, ENTRANCES_TO_CAR, ROPES, ROPE_SIZE, LIMITED, BILL_CODE, COMMENTS, BLD_ELEV_NBR) ***Number of Records = 25,989***

ELEV_ELEVATOR_SUMMARY (INSPECTION_DATE, INVOICE, STATE_ID, FEE, PAID_DATE, INSPECTION_TYPE, INSPECTOR_CODE, CERTIFICATE_STATUS, LIMITED, WRITE_OFF, NBR_VIOLATIONS) ***Number of Records = 416,890***

ELEV_IMAGE_ELEV_INSP (INVOICE, STATE_ID, COUNTY_CODE, COUNTY_AREA, ELEVATOR_TYPE, OPERATION_TYPE, CAPACITY, INSTALLED_DATE, COMPLIED_DATE, STATE_OWN, OWNER_CODE*, OCCUPANT_CODE*, EQUIPMENT_TYPE*, DRIVE_MACHINE, VOLTS, SPEED, FLOOR_FROM, FLOOR_TO, ENTRANCES_TO_CAR, ROPES, ROPE_SIZE, LIMITED, BILL_CODE, COMMENTS, BLD_ELEV_NBR, O_NAME_CODE*, O_NAME, O_ADDRESS1, O_ADDRESS2, O_CITY, O_STATE, O_ZIP_CODE, O_TITLE, O_F_NM, O_L_NM, O_NAME2, O_EMAIL, O_PHONE, O_FAX, U_NAME_CODE*, U_NAME, U_ADDRESS1, U_ADDRESS2, U_CITY, U_STATE, U_ZIP_CODE, U_TITLE, U_F_NM, U_L_NM, U_NAME2, U_EMAIL, U_PHONE, U_FAX, INSPECTION_DATE, FEE, PAID_DATE, INSPECTION_TYPE, INSPECTOR_CODE*,

CERTIFICATE_STATUS, ABATE_DATE, POINTED_OUT, STATUS, REPORT_NBR, STMT_NBR, B_NAME_CODE*, B_NAME, B_ADDRESS1, B_ADDRESS2, B_CITY, B_STATE, B_ZIP_CODE, B_TITLE, B_F_NM, B_L_NM, B_NAME2, B_EMAIL, B_PHONE, B_FAX) ***Number of Records = 76,458***

ELEV_IMAGE_VIOLS (INVOICE, STATE_ID, SECTION_RULE, VIO_TEXT) ***Number of Records = 122,065***

ELEV_INSPECTIONS (INVOICE, INSPECTION_DATE, FEE, PAID_DATE, INSPECTION_TYPE, INSPECTOR_CODE*, CERTIFICATE_STATUS, LIMITED, LAST_INSPECTED_INDICATOR, WRITE_OFF, WRITE_OFF_CD, WRITE_OFF_AMT, INVOICE_DATE, LETTER2_DATE, LETTER3_DATE, PHONE_CONTACT_DATE, PROMISE_PAY_DATE, ABATE_DATE, POINTED_OUT, NSF_FEE, REPORT_NBR, STMT_NBR) ***Number of Records = 416,890***

ELEV_INSPECTOR (INSPECTOR_CODE, TITLE, F_NAME, M_NAME, L_NAME, COMP_NAME, STREET, PO_BOX, CITY, STATE, ZIP, SUPERV_CODE*, EMAIL) ***Number of Records = 53***

ELEV_NBR_VIOLATIONS (INVOICE, CNT_VIOLATIONS) ***Number of Records = 416,123***

ELEV_NEW_ALT_LOG (ID_NBR, STATE_ID*, COMPLIED_DATE, ELEVATOR_TYPE, COUNTY_CODE, COUNTY_AREA, OPERATION_TYPE, CAPACITY, DATE_ENTERED, DATE_EXPIRES, LANDINGS, ENTRANCES_TO_CAR, AMT, ROPES, ROPE_SIZE, EQUIPMENT_TYPE, DRIVE_MACHINE, VOLTS, FLOOR_FROM, FLOOR_TO, SPEED, SCOPE_WORK, COMMENTS, APPLICANT_CODE*, OWNER_CODE*, OCCUPANT_CODE*, STATUS, CLOSING_INVOICE, BLD_ELEV_NBR, PAYMT_RECD_DATE, PAYMT_TYPE, BILL_CODE) ***Number of Records = 7589***

ELEV_NEW_ELEVATOR_LOG (ID, MONTH, YEAR, NAME, LOC, TYPE, AMT, CODE, SUB_CODE, COUNTY_CODE, OPEN, DATE_ENTERED) ***Number of Records = 11,249***

ELEV_TRANSMITTAL_POOL (INVOICE, COMPANY_NAME, CHECK_DATE, CHECK_NUMBER, FEE, DATE_ENTERED, DATE_POSTED, DATE_MATCHED, POSTED_FLAG, BATCH_NUMBER, NSF_FEE, STMT_NBR, REPORT_NBR) ***Number of Records = 232,954***

ELEV_UPDTE_HISTORY (CHG_DTE, INSPECTOR_CODE*, STATE_ID, INVOICE, TBL, CHG, REPORT_NBR) ***Number of Records = 40,736***

ELEV_VIOLATIONS (INVOICE, STATE_ID, SECTION_RULE, VIO_TEXT) ***Number of Records = 813,404***

XIV. Out of Scope

A comprehensive list of out-of-scope elements will be defined during the initial business analysis performed by the awarded vendor.